McAfee®

Internet Security

Guida dell'utente

Sommario

CAPITOLO 1

McAfee Internet Security

Analogamente a un sistema di protezione per il computer, Internet Security protegge tutta la famiglia dalle minacce più recenti e, al contempo, rende più sicura l'esperienza online. Internet Security può essere utilizzato per proteggere il computer da virus, hacker e spyware, per controllare il traffico Internet per individuare attività sospette, per proteggere la privacy della famiglia, per valutare siti Web rischiosi e molto altro ancora.

In questo capitolo

CAPITOLO 2

McAfee SecurityCenter

McAfee SecurityCenter consente di monitorare lo stato della protezione del computer, stabilire immediatamente se i servizi di protezione del computer relativi a virus, spyware, posta elettronica e firewall sono aggiornati e intervenire sulle eventuali vulnerabilità dei sistemi di protezione utilizzati. Fornisce inoltre gli strumenti e i controlli di navigazione necessari per coordinare e gestire tutte le aree di protezione del computer.

Prima di iniziare a configurare e gestire la protezione del computer, è opportuno esaminare l'interfaccia di SecurityCenter e assicurarsi di comprendere la differenza tra stato della protezione, categorie di protezione e servizi di protezione. Quindi, per assicurarsi di avere a disposizione la protezione McAfee più recente, è necessario aggiornare SecurityCenter.

Dopo aver completato le attività iniziali di configurazione, utilizzare SecurityCenter per monitorare lo stato della protezione del computer. Nel caso in cui rilevi un problema di protezione, SecurityCenter lo segnala per consentire all'utente di risolverlo o ignorarlo, in base alla gravità. È anche disponibile un registro eventi in cui è possibile esaminare gli eventi di SecurityCenter, ad esempio eventuali modifiche di configurazione della scansione antivirus.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

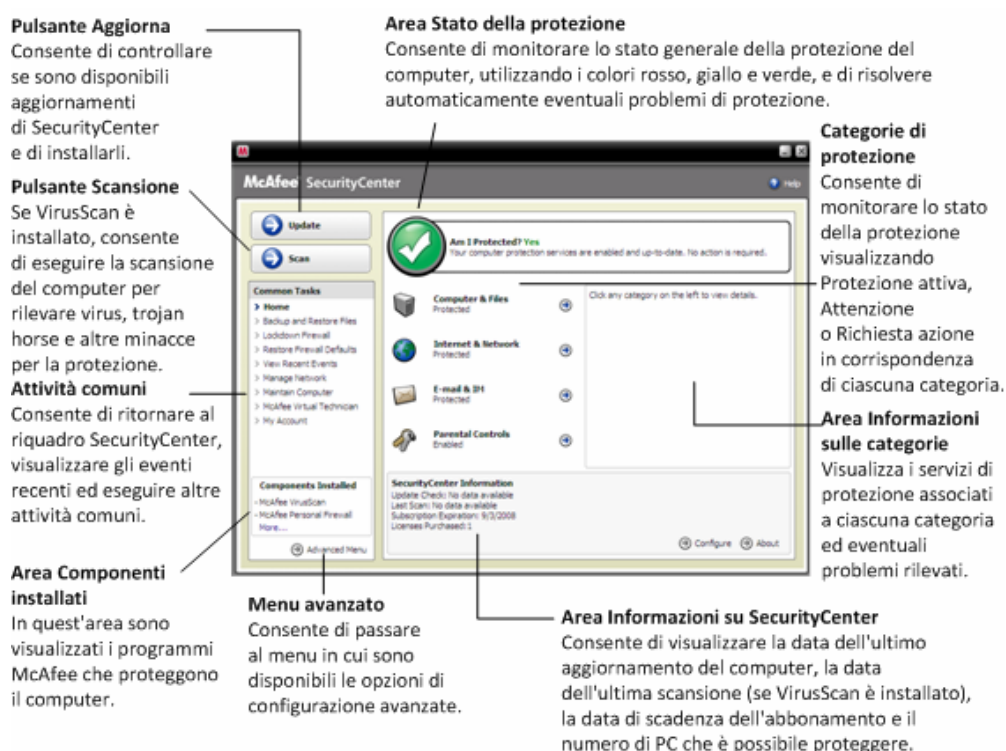
In questo capitolo

Funzioni di SecurityCenter

Stato di protezione semplificato	Consente un controllo semplificato dello stato della protezione del computer, la verifica della disponibilità di aggiornamenti e la risoluzione dei problemi di protezione.
Aggiornamenti automatici	SecurityCenter esegue automaticamente il download e l'installazione degli aggiornamenti dei programmi. Le nuove versioni dei programmi McAfee vengono automaticamente distribuite al computer in uso non appena risultano disponibili, purché l'abbonamento sia valido, in modo tale da garantire una protezione sempre aggiornata.
Avvisi in tempo reale	Gli avvisi di protezione notificano all'utente la presenza di epidemie di virus e di minacce per la protezione.

CAPITOLO 3

Utilizzo di SecurityCenter

Prima di iniziare a utilizzare SecurityCenter, esaminare i componenti e le aree di configurazione da utilizzare per gestire lo stato della protezione del computer. Per ulteriori informazioni sulla terminologia utilizzata nell'immagine, vedere le sezioni Informazioni sullo stato della protezione (pagina 8) e Informazioni sulle categorie di protezione (pagina 9). Esaminare quindi le informazioni relative al proprio account McAfee e verificare la validità del proprio abbonamento.

In questo capitolo

Informazioni sullo stato della protezione

Lo stato della protezione del computer in uso è riportato in un'apposita area del riquadro SecurityCenter. Lo stato indica se il computer è completamente protetto contro le minacce per la protezione più recenti e se può subire gli effetti causati, ad esempio, da un attacco informatico esterno, da un altro programma di protezione o da un programma che accede a Internet.

Lo stato della protezione del computer può essere rosso, giallo o verde.

Stato della protezione	Descrizione
Rosso	Il computer non è protetto. L'area dello stato della protezione del riquadro SecurityCenter è rossa e indica che il computer non è protetto. SecurityCenter segnala la presenza di almeno un problema critico di protezione. Per ottenere una protezione completa, è necessario risolvere tutti i problemi critici in ciascuna categoria di protezione. Lo stato della categoria del problema, anch'esso visualizzato in rosso, è impostato su **Necessaria azione**. Per informazioni su come risolvere i problemi di protezione, consultare la sezione Risoluzione dei problemi di protezione (pagina 18).
Giallo	Il computer è parzialmente protetto. L'area dello stato della protezione del riquadro SecurityCenter è gialla e indica che il computer non è protetto. SecurityCenter segnala la presenza di almeno un problema non critico di protezione. Per ottenere una protezione completa, è necessario risolvere o ignorare i problemi non critici associati a ogni categoria di protezione. Per informazioni su come risolvere o ignorare i problemi di protezione, vedere Risoluzione o esclusione dei problemi di protezione (pagina 17).
Verde	Il computer è completamente protetto. L'area dello stato della protezione del riquadro SecurityCenter è verde e indica che il computer è protetto. SecurityCenter non segnala alcun problema di protezione critico o non critico. In ogni categoria di protezione sono elencati i servizi che proteggono il computer.

Informazioni sulle categorie di protezione

I servizi di protezione di SecurityCenter sono suddivisi in quattro categorie: Computer e file, Internet e rete, Posta elettronica e MI e Controllo genitori. Queste categorie consentono di identificare e configurare i servizi di protezione del computer.

Per configurare i servizi di protezione di una determinata categoria e visualizzare i problemi di protezione rilevati per tali servizi, è sufficiente fare clic sulla categoria. Se lo stato di protezione del computer è rosso o giallo, per una o più categorie viene visualizzato il messaggio *Necessaria azione* o *Attenzione*, che indica che SecurityCenter ha rilevato un problema all'interno della categoria. Per ulteriori informazioni sullo stato della protezione, consultare la sezione Informazioni sullo stato della protezione (pagina 8).

Categoria di protezione	Descrizione
Computer e file	La categoria Computer e file consente di configurare i seguenti servizi di protezione: ▪ Protezione da virus ▪ Protezione da spyware ▪ SystemGuards ▪ Protezione di Windows ▪ Stato del computer
Internet e rete	La categoria Internet e rete consente di configurare i seguenti servizi di protezione: ▪ Protezione firewall ▪ Protezione da phishing ▪ Protezione dell'identità
Posta elettronica e MI	La categoria Posta elettronica e MI consente di configurare i seguenti servizi di protezione: ▪ Protezione da virus posta elettronica ▪ Protezione MI da virus ▪ Protezione posta elettronica da spyware ▪ Protezione MI da spyware ▪ Protezione da posta indesiderata
Controllo genitori	La categoria Controllo genitori consente di configurare i seguenti servizi di protezione: ▪ Blocco contenuti

Informazioni sui servizi di protezione

I servizi di protezione rappresentano i vari componenti da configurare per proteggere il computer e i file. Ogni servizio di protezione corrisponde direttamente a un programma McAfee. Quando si installa il programma VirusScan, ad esempio, nel sistema vengono attivati i seguenti servizi di protezione: protezione da virus, protezione da spyware, SystemGuards e scansione script. Per ottenere informazioni dettagliate su questi servizi di protezione, consultare la Guida di VirusScan.

Quando si installa un programma, tutti i servizi di protezione ad esso associati vengono attivati per impostazione predefinita. I servizi di protezione possono tuttavia essere disattivati in qualsiasi momento. Se ad esempio si installa Parental Controls, i servizi Blocco contenuti e Protezione dell'identità vengono entrambi attivati. Se non si desidera utilizzare il servizio di protezione Blocco contenuti, è possibile disattivarlo completamente. È anche possibile disattivare temporaneamente un servizio di protezione durante l'esecuzione di attività di configurazione o di manutenzione.

Gestione degli abbonamenti

Ogni prodotto McAfee acquistato è accompagnato da un abbonamento che consente di utilizzare il prodotto su un determinato numero di computer per un determinato periodo di tempo. La durata dell'abbonamento varia in base all'acquisto, ma in genere inizia quando il prodotto viene attivato. L'attivazione è semplice e gratuita: occorre soltanto una connessione a Internet, ma è molto importante in quanto dà diritto a ricevere gli aggiornamenti periodici e automatici del prodotto, che consentono di mantenere il computer protetto dalle minacce più recenti.

L'attivazione in genere avviene quando il prodotto viene installato, tuttavia, se si decide di rimandarla, ad esempio perché non si dispone di una connessione a Internet, è possibile effettuarla entro 15 giorni. Se non si effettua l'attivazione entro 15 giorni, i prodotti non riceveranno gli aggiornamenti fondamentali né eseguiranno le scansioni. L'utente viene inoltre informato periodicamente, tramite messaggi visualizzati sullo schermo, dell'imminente scadenza dell'abbonamento. In questo modo è possibile evitare interruzioni della protezione rinnovando l'abbonamento in anticipo o impostando il rinnovo automatico nel sito Web di McAfee.

Se in SecurityCenter viene visualizzato un collegamento che richiede di eseguire l'attivazione, significa che l'abbonamento non è stato attivato. Per visualizzare la data di scadenza dell'abbonamento, è possibile controllare la pagina dell'account.

Come accedere all'account McAfee

SecurityCenter consente di accedere facilmente alle informazioni relative al proprio account McAfee.

1. Nella sezione **Attività comuni**, fare clic su **Account**.
2. Accedere al proprio account McAfee.

Come attivare il prodotto

L'attivazione in genere avviene quando si installa il prodotto, in caso contrario viene visualizzato un collegamento in SecurityCenter che richiede di eseguire l'attivazione. L'utente riceve inoltre notifiche periodiche.

- Nella sezione **Informazioni su SecurityCenter** del riquadro Home di SecurityCenter, fare clic su **Attivare l'abbonamento**.

Suggerimento: è inoltre possibile attivare l'abbonamento dall'avviso visualizzato periodicamente.

Come verificare l'abbonamento

È necessario verificare il proprio abbonamento per accertarsi che non sia scaduto.

- Fare clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica, all'estremità destra della barra delle applicazioni, quindi scegliere **Verifica abbonamento**.

Come rinnovare l'abbonamento

Poco prima della scadenza dell'abbonamento, viene visualizzato un collegamento in SecurityCenter che richiede di rinnovare l'abbonamento. McAfee avverte inoltre periodicamente dell'imminente scadenza tramite degli avvisi.

- Nella sezione **Informazioni su SecurityCenter** del riquadro Home di SecurityCenter, fare clic su **Rinnova**.

Suggerimento: è inoltre possibile rinnovare l'abbonamento dal messaggio di notifica che viene visualizzato periodicamente. In alternativa, andare alla pagina dell'account in cui è possibile effettuare il rinnovo o impostare il rinnovo automatico.

CAPITOLO 4

Aggiornamento di SecurityCenter

Per garantire che i programmi McAfee registrati in uso siano sempre aggiornati, SecurityCenter verifica ogni quattro ore la disponibilità di aggiornamenti in linea ed eventualmente li installa. In base ai programmi installati e attivati, gli aggiornamenti in linea possono includere le definizioni più recenti dei virus nonché gli aggiornamenti della protezione della privacy o da hacker, posta indesiderata e spyware. È possibile verificare la disponibilità di aggiornamenti in qualsiasi momento durante l'intervallo predefinito di quattro ore. Mentre SecurityCenter verifica la disponibilità di aggiornamenti, è possibile proseguire con altre attività.

Benché non sia consigliato, è possibile modificare la modalità con cui SecurityCenter verifica e installa gli aggiornamenti. Ad esempio, è possibile configurare SecurityCenter in modo tale da scaricare ma non installare gli aggiornamenti o per ricevere una notifica prima di eseguire il download o l'installazione degli aggiornamenti. È inoltre possibile disattivare l'aggiornamento automatico.

Nota: se il prodotto McAfee è stato installato da un CD, è necessario effettuare l'attivazione entro 15 giorni, in caso contrario i prodotti non riceveranno aggiornamenti fondamentali né eseguiranno scansioni.

In questo capitolo

Come verificare la disponibilità di aggiornamenti

Per impostazione predefinita, quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, tuttavia è possibile effettuare manualmente la verifica durante l'intervallo di quattro ore. Se gli aggiornamenti automatici sono stati disattivati, è responsabilità dell'utente verificare periodicamente la disponibilità di aggiornamenti.

- Nel riquadro SecurityCenter, fare clic su **Aggiorna**.

Suggerimento: per verificare la disponibilità di aggiornamenti senza avviare SecurityCenter, è possibile fare clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica all'estremità destra della barra delle applicazioni e quindi fare clic su **Aggiornamenti**.

Come configurare gli aggiornamenti automatici

Per impostazione predefinita, quando si è connessi a Internet, SecurityCenter esegue automaticamente la ricerca e l'installazione degli aggiornamenti ogni quattro ore. Se si desidera modificare il funzionamento predefinito, è possibile configurare SecurityCenter in modo tale che esegua automaticamente il download degli aggiornamenti e quindi visualizzi un avviso quando gli aggiornamenti sono pronti per l'installazione o per ricevere una notifica prima di scaricare gli aggiornamenti.

Nota: SecurityCenter indica che gli aggiornamenti sono pronti per essere scaricati o installati mediante un avviso. In base all'avviso è possibile scaricare, installare o posticipare gli aggiornamenti. Quando si aggiorna un programma a partire da un avviso, è possibile che venga richiesto di verificare l'abbonamento prima di procedere al download e all'installazione. Per ulteriori informazioni, vedere Utilizzo degli avvisi (pagina 21).

1 Aprire il riquadro di configurazione di SecurityCenter.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

2 Nel riquadro di configurazione di SecurityCenter, in **Gli aggiornamenti automatici non sono attivi**, fare clic su **Attiva** e quindi su **Avanzate**.

3 Fare clic su uno dei seguenti pulsanti:

   - **Installa automaticamente gli aggiornamenti e avvisa quando i servizi vengono aggiornati (consigliato)**
   - **Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione**
   - **Avvisa prima di scaricare aggiornamenti**

4 Fare clic su **OK**.

Come disattivare gli aggiornamenti automatici

Se si disattivano gli aggiornamenti automatici, l'utente dovrà verificare periodicamente la disponibilità di aggiornamenti per assicurarsi che il computer disponga della protezione più aggiornata. Per informazioni sulla verifica manuale della disponibilità di aggiornamenti, vedere Come verificare la disponibilità di aggiornamenti (pagina 13).

1 Aprire il riquadro di configurazione di SecurityCenter.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

2 Nel riquadro di configurazione di SecurityCenter, in **Gli aggiornamenti automatici sono attivi**, fare clic su **Disattiva**.

3 Nella finestra di dialogo di conferma, fare clic su **Sì**.

Suggerimento: per attivare gli aggiornamenti automatici, fare clic sul pulsante **Attiva** o deselezionare l'opzione **Disattiva l'aggiornamento automatico e consenti la ricerca manuale di aggiornamenti** nel riquadro Opzioni di aggiornamento.

CAPITOLO 5

Risoluzione o esclusione dei problemi di protezione

SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. I problemi critici di protezione richiedono un intervento immediato e comportano il passaggio dello stato della protezione a rosso. I problemi non critici di protezione non richiedono un intervento immediato e, a seconda del tipo di problema, possono influire sullo stato della protezione. Per raggiungere uno stato della protezione verde, è necessario risolvere tutti i problemi critici e risolvere oppure ignorare tutti i problemi non critici. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee. Per ulteriori informazioni sul tecnico virtuale di McAfee, consultare la relativa Guida.

In questo capitolo

Risoluzione dei problemi di protezione

Nella maggior parte dei casi, i problemi di protezione possono essere risolti automaticamente, tuttavia alcuni problemi richiedono un intervento manuale. Se ad esempio la funzione Protezione firewall è disattivata, SecurityCenter può attivarla automaticamente, ma se la funzione non è installata, sarà necessario installarla. Nella tabella seguente sono riportate alcune altre azioni che è possibile intraprendere per risolvere manualmente i problemi di protezione:

Problema	Azione
Non è stata eseguita alcuna scansione completa negli ultimi 30 giorni.	Eseguire una scansione manuale del computer. Per ulteriori informazioni, consultare la Guida di VirusScan.
I file delle firme per i rilevamenti (DAT) non sono aggiornati.	Aggiornare manualmente la protezione. Per ulteriori informazioni, consultare la Guida di VirusScan.
Un programma non è stato installato.	Installare il programma dal sito Web di McAfee o da CD.
Un programma non presenta tutti i componenti necessari.	Reinstallare il programma dal sito Web di McAfee o da CD.
Un programma non è stato attivato e non può ricevere tutti i servizi di protezione.	Attivare il programma sul sito Web di McAfee.
Abbonamento scaduto.	Verificare lo stato del proprio account sul sito Web di McAfee. Per ulteriori informazioni, vedere Gestione degli abbonamenti (pagina 11).

Nota: spesso un unico problema di protezione influisce su più categorie di protezione. In questo caso, se il problema viene risolto per una categoria, verrà risolto anche per tutte le altre categorie di protezione.

Risoluzione automatica dei problemi di protezione

SecurityCenter è in grado di risolvere automaticamente la maggior parte dei problemi di protezione. Le modifiche apportate da SecurityCenter alla configurazione durante la risoluzione automatica dei problemi di protezione non vengono aggiunte nel registro eventi. Per ulteriori informazioni sugli eventi, consultare la sezione Visualizzazione degli eventi (pagina 27).

1 Nella sezione **Attività comuni**, fare clic su **Home**.

2 Nel riquadro SecurityCenter, nell'area dello stato della protezione, fare clic su **Correggi**.

Come risolvere manualmente i problemi di protezione

Se uno o più problemi di protezione non vengono risolti tramite la procedura automatica, è possibile intervenire manualmente.

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic sulla categoria di protezione per cui SecurityCenter ha rilevato il problema.
3. Fare clic sul collegamento accanto alla descrizione del problema.

Esclusione dei problemi di protezione

Se SecurityCenter rileva un problema non critico è possibile risolverlo o ignorarlo. Alcuni problemi non critici, ad esempio se Anti-Spam o Parental Controls non è installato, vengono automaticamente ignorati. I problemi ignorati vengono riportati nell'area delle informazioni sulle categorie di protezione del riquadro Home di SecurityCenter solo se lo stato della protezione del computer è verde. Se un problema viene ignorato e successivamente si decide di visualizzarlo nell'area delle informazioni sulle categorie di protezione anche se lo stato della protezione non è verde, sarà possibile visualizzarlo.

Come ignorare un problema di protezione

Se SecurityCenter rileva un problema non critico che non si desidera risolvere, è possibile ignorarlo. I problemi ignorati vengono rimossi dall'area delle informazioni sulle categorie di protezione di SecurityCenter.

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic sulla categoria di protezione per cui il problema è stato rilevato.
3. Fare clic sul collegamento **Ignora** accanto al problema di protezione.

Come visualizzare o nascondere i problemi ignorati

In base alla gravità, i problemi di protezione possono essere visualizzati o nascosti.

1 Aprire il riquadro Opzioni di avviso.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
   3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Configurazione di SecurityCenter, fare clic su **Problemi ignorati**.

3 Nel riquadro Problemi ignorati, effettuare le seguenti operazioni:

   - Per ignorare un problema, selezionare la relativa casella di controllo.
   - Per visualizzare un problema nell'area delle informazioni sulle categorie di protezione, deselezionare la relativa casella di controllo.

4 Fare clic su **OK**.

Suggerimento: per ignorare un problema è anche possibile fare clic sul collegamento **Ignora** accanto al problema rilevato nell'area delle informazioni sulle categorie di protezione.

CAPITOLO 6

Utilizzo degli avvisi

Gli avvisi sono piccole finestre popup che vengono visualizzate nell'angolo inferiore destro dello schermo quando si verificano determinati eventi di SecurityCenter. Un avviso fornisce informazioni dettagliate su un evento, oltre a consigli e opzioni per la risoluzione dei problemi che possono essere associati a tale evento. Alcuni avvisi contengono inoltre dei collegamenti a informazioni aggiuntive sull'evento. Tali collegamenti reindirizzano l'utente al sito Web globale di McAfee oppure consentono di inviare informazioni a McAfee per la risoluzione dei problemi.

Esistono tre tipi di avvisi: rosso, giallo e verde.

Tipo di avviso	Descrizione
Rosso	Un avviso rosso è una notifica critica che richiede una risposta da parte dell'utente. Gli avvisi rossi vengono visualizzati quando SecurityCenter non è in grado di individuare automaticamente la risoluzione di un problema di protezione.
Giallo	Un avviso giallo è una notifica non critica che di solito richiede una risposta da parte dell'utente.
Verde	Un avviso verde è una notifica non critica che non richiede una risposta da parte dell'utente. Gli avvisi verdi forniscono informazioni di base su un evento.

Non è possibile disabilitare gli avvisi, poiché hanno un ruolo chiave nel monitoraggio e nella gestione dello stato di protezione. Tuttavia, è possibile impostare la visualizzazione di determinati tipi di avvisi informativi e configurare altre opzioni di avviso (ad esempio, se SecurityCenter deve riprodurre un suono quando viene visualizzato un avviso oppure se visualizzare la schermata iniziale di McAfee all'avvio).

In questo capitolo

Mostrare e nascondere gli avvisi informativi

Gli avvisi informativi avvisano l'utente quando si verificano degli eventi che non rappresentano una minaccia per la protezione del computer. Ad esempio, se è stata impostata la Protezione firewall, per impostazione predefinita verrà visualizzato un avviso informativo ogni volta che un programma installato sul computer viene autorizzato all'accesso a Internet. Qualora non si desideri che venga visualizzato un tipo specifico di avviso informativo, è possibile nasconderlo. Se non si desidera che venga visualizzato alcun avviso, è possibile nasconderli tutti. È inoltre possibile nascondere tutti gli avvisi informativi quando si esegue un gioco in modalità a schermo intero sul computer. Al termine del gioco, quando si esce dalla modalità a schermo intero, SecurityCenter riprende la visualizzazione degli avvisi informativi.

Se si nasconde per errore un avviso informativo, sarà possibile visualizzarlo di nuovo in qualsiasi momento. Per impostazione predefinita, SecurityCenter mostra tutti gli avvisi informativi.

Come mostrare o nascondere gli avvisi informativi

È possibile configurare SecurityCenter in modo da mostrare alcuni avvisi informativi e nasconderne altri, oppure nascondere tutti gli avvisi informativi.

1 Aprire il riquadro Opzioni di avviso.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
   3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi informativi**.

3 Nel riquadro Avvisi informativi, effettuare le seguenti operazioni:

- Per visualizzare un avviso informativo, deselezionare la relativa casella di controllo.
- Per nascondere un avviso informativo, selezionare la relativa casella di controllo.
- Per nascondere tutti gli avvisi informativi, selezionare la casella di controllo **Non visualizzare avvisi informativi**.

4 Fare clic su **OK**.

Suggerimento: è inoltre possibile nascondere un avviso informativo selezionando la casella di controllo **Non visualizzare questo messaggio in futuro** nella finestra dell'avviso stesso. In tal modo, sarà possibile visualizzare nuovamente l'avviso informativo deselezionando la casella di controllo appropriata nel riquadro Avvisi informativi.

Come mostrare o nascondere gli avvisi informativi durante una sessione di gioco

È possibile nascondere gli avvisi informativi quando si esegue un gioco in modalità a schermo intero sul computer. Al termine del gioco, quando si esce dalla modalità a schermo intero, SecurityCenter riprende la visualizzazione degli avvisi informativi.

1 Aprire il riquadro Opzioni di avviso.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
   3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Opzioni di avviso, selezionare o deselezionare la casella di controllo **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**.

3 Fare clic su **OK**.

Configurazione delle opzioni di avviso

L'aspetto e la frequenza degli avvisi vengono configurati da SecurityCenter; tuttavia, l'utente può modificare alcune opzioni di avviso di base. Ad esempio, è possibile riprodurre un suono quando vengono visualizzati gli avvisi oppure nascondere l'avviso della schermata iniziale all'avvio di Windows. È inoltre possibile nascondere gli avvisi che avvertono gli utenti di epidemie di virus e altre minacce per la protezione nella community online.

Come riprodurre un suono con gli avvisi

Se si desidera ricevere un segnale acustico quando si verifica un avviso, è possibile configurare SecurityCenter in modo da riprodurre un suono al verificarsi di ciascun avviso.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel pannello Opzioni di avviso, nella sezione **Audio**, selezionare la casella di controllo **Riproduci un suono quando si verifica un avviso**.

Come nascondere la schermata iniziale all'avvio

Per impostazione predefinita, la schermata iniziale di McAfee viene visualizzata brevemente all'avvio di Windows per avvisare l'utente che sul computer è attiva la protezione offerta da SecurityCenter. È tuttavia possibile nascondere la schermata iniziale qualora non si desideri che venga visualizzata.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel pannello Opzioni di avviso, nella sezione **Schermata iniziale**, deselezionare la casella di controllo **Mostra la schermata iniziale di McAfee all'avvio di Windows**.

Suggerimento: è possibile mostrare nuovamente la schermata iniziale in qualsiasi momento selezionando la casella di controllo **Mostra la schermata iniziale di McAfee all'avvio di Windows**.

Come nascondere gli avvisi sulle epidemie di virus

È possibile nascondere gli avvisi che notificano agli utenti epidemie di virus e altre minacce per la protezione nella community online.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Opzioni di avviso, deselezionare la casella di controllo **Avvisa quando viene rilevato un virus o una minaccia per la protezione**.

Suggerimento: è possibile mostrare gli avvisi sulle epidemie di virus in qualsiasi momento selezionando la casella di controllo **Avvisa quando viene rilevato un virus o una minaccia per la protezione**.

Come nascondere i messaggi sulla protezione

È possibile nascondere le notifiche relative alla protezione di più computer della rete domestica. Tali messaggi forniscono informazioni relative all'abbonamento, al numero di computer che è possibile proteggere mediante l'abbonamento e all'estensione dell'abbonamento per proteggere ulteriori computer.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Opzioni di avviso deselezionare la casella di controllo **Mostra avvisi su virus o altri messaggi sulla protezione**.

Suggerimento: è possibile visualizzare tali avvisi in qualsiasi momento selezionando la casella di controllo **Mostra avvisi su virus o altri messaggi sulla protezione**.

CAPITOLO 7

Visualizzazione di eventi

Un evento è un'azione o una modifica della configurazione che si verifica nell'ambito di una categoria di protezione e i relativi servizi di protezione. Diversi servizi di protezione registrano tipi di eventi differenti. Ad esempio, SecurityCenter registra un evento se si attiva o disattiva un servizio di protezione; Virus Protection registra un evento ogni volta che un virus viene rilevato e rimosso; Firewall Protection registra un evento ogni volta che viene bloccato un tentativo di connessione a Internet. Per ulteriori informazioni sulle categorie di protezione, vedere Informazioni sulle categorie di protezione (pagina 9).

È possibile visualizzare eventi durante la risoluzione dei problemi di configurazione e la revisione delle operazioni eseguite da altri utenti. Molti genitori utilizzano il registro eventi per monitorare il comportamento dei propri figli su Internet. È possibile visualizzare gli eventi recenti se si desidera esaminare solo gli ultimi 30 eventi verificatisi, tutti gli eventi se si desidera esaminare un elenco completo di tutti gli eventi verificatisi. Quando si visualizzano tutti gli eventi, SecurityCenter avvia il registro eventi, in cui gli eventi sono ordinati in base alla categoria di protezione nell'ambito della quale si sono verificati.

In questo capitolo

Visualizzazione degli eventi recenti

È possibile visualizzare gli eventi recenti se si desidera esaminare solo gli ultimi 30 eventi verificatisi.

- Nella sezione **Attività comuni**, fare clic su **Visualizza eventi recenti**.

Come visualizzare tutti gli eventi

È possibile visualizzare tutti gli eventi se si desidera esaminare un elenco completo di tutti gli eventi verificatisi.

1. Nella sezione **Attività comuni**, fare clic su **Visualizza eventi recenti**.
2. Nel riquadro Eventi recenti, fare clic su **Visualizza registro**.
3. Nel riquadro a sinistra del registro eventi, fare clic sul tipo di eventi che si desidera visualizzare.

CAPITOLO 8

McAfee VirusScan

I servizi di rilevamento e protezione avanzati di VirusScan difendono i dati e il computer dell'utente dalle minacce più recenti per la protezione, da virus, trojan horse, cookie che registrano le informazioni, spyware, adware e altri programmi potenzialmente indesiderati. La protezione si estende oltre i file e le cartelle sul desktop, puntando alle minacce provenienti da diversi punti d'accesso, tra cui messaggi di posta elettronica, messaggi immediati e il Web.

Con VirusScan, la protezione del computer è immediata e costante e non richiede tediose procedure amministrative. Mentre l'utente lavora, gioca, naviga sul Web o controlla la posta elettronica, VirusScan viene eseguito in background, controllando, analizzando e rilevando i danni potenziali in tempo reale. Il software pianifica scansioni complete periodiche del computer, utilizzando una gamma più complessa di opzioni. Grazie alla sua flessibilità, VirusScan offre all'utente la possibilità di personalizzare questo funzionamento, se lo desidera; in caso contrario, il computer resta comunque protetto.

Con il normale utilizzo, virus, worm e altre minacce potenziali possono infiltrarsi nel computer. In questo caso, VirusScan avvisa l'utente della minaccia, ma la gestisce in sua vece, pulendo o mettendo in quarantena gli elementi infetti prima che si verifichi qualsiasi danno. In rari casi, potrebbero essere necessarie alcune ulteriori operazioni. In questa eventualità, VirusScan consente all'utente di decidere sul da farsi: eseguire una nuova scansione al successivo avvio del computer, mantenere l'elemento rilevato oppure rimuoverlo.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di VirusScan

Estesa protezione antivirus

Consente di proteggere l'utente e il computer dalle minacce alla protezione più recenti, inclusi virus, Trojan, tracking cookie, spyware, adware e altri programmi potenzialmente indesiderati. La protezione si estende oltre i file e le cartelle sul desktop, puntando alle minacce provenienti da diversi punti d'accesso, tra cui messaggi di posta elettronica, messaggi immediati e il Web. Non sono necessarie tediose procedure amministrative.

Opzioni di scansione in funzione delle risorse

Se lo si desidera è possibile personalizzare le opzioni di scansione, ma anche se ciò non avviene il computer rimane protetto. Se si riscontrano problemi di lentezza della scansione, è possibile disattivare l'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo presente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività.

Riparazioni automatiche

Se VirusScan rileva una minaccia per la protezione durante l'esecuzione di una scansione, tenterà di gestirla automaticamente in base al tipo di minaccia. In tal modo, è possibile rilevare e neutralizzare gran parte delle minacce senza l'interazione dell'utente. In rari casi, VirusScan può non essere in grado di neutralizzare autonomamente una minaccia. In questa eventualità, VirusScan consente all'utente di decidere sul da farsi: eseguire una nuova scansione al successivo avvio del computer, mantenere l'elemento rilevato oppure rimuoverlo.

Sospensione delle attività in modalità a schermo intero

Quando sul computer si riproducono film, videogiochi o si eseguono altre applicazioni che occupano l'intero schermo, VirusScan sospende alcune attività, quali ad esempio le scansioni manuali.

CAPITOLO 9

Scansione del computer

Ancora prima di avviare SecurityCenter per la prima volta, la protezione da virus in tempo reale di VirusScan inizia a proteggere il computer da virus potenzialmente dannosi, Trojan e altre minacce per la protezione. A meno che non si disattivi la protezione da virus in tempo reale, VirusScan monitora costantemente il computer per rilevare la presenza di eventuali attività di virus, eseguendo la scansione dei file a ogni accesso da parte dell'utente o del computer e utilizzando le opzioni di scansione in tempo reale impostate. Per garantire la protezione del computer dalle più recenti minacce per la protezione, lasciare attivata la protezione da virus in tempo reale e impostare una pianificazione per l'esecuzione di scansioni manuali periodiche più approfondite. Per ulteriori informazioni sull'impostazione delle opzioni di scansione, consultare Impostazione della protezione da virus (pagina 47).

VirusScan offre una serie di opzioni di scansione più dettagliate per la protezione antivirus, consentendo all'utente di eseguire periodicamente scansioni più approfondite. In SecurityCenter è possibile eseguire una scansione completa, rapida, personalizzata o pianificata. È anche possibile eseguire scansioni manuali in Esplora risorse senza interrompere le altre attività. La scansione in SecurityCenter offre il vantaggio di modificare immediatamente le opzioni di scansione. Tuttavia, la scansione da Esplora risorse offre un approccio comodo alla protezione del computer.

Se si esegue una scansione da SecurityCenter o da Esplora risorse, al termine è comunque possibile visualizzarne i risultati. La visualizzazione dei risultati di una scansione consente di determinare se VirusScan ha rilevato, riparato o messo in quarantena virus, Trojan, spyware, adware, cookie e altri programmi potenzialmente indesiderati. I risultati di una scansione possono essere visualizzati in modo differente. Ad esempio è possibile visualizzare un riepilogo di base dei risultati della scansione o informazioni dettagliate quali lo stato e il tipo di infezione nonché statistiche generali sulla scansione e sul rilevamento.

In questo capitolo

Come analizzare il PC

VirusScan offre una serie completa di opzioni di scansione per la protezione antivirus, inclusa la scansione in tempo reale, che monitora costantemente il computer per rilevare la presenza di eventuali attività di minaccia, la scansione manuale da Esplora risorse e la scansione completa, rapida, personalizzata o pianificata da SecurityCenter.

Per...	Procedere come segue...
Avviare la scansione in tempo reale in modo da controllare costantemente il computer per rilevare la presenza di eventuali attività di virus, analizzando i file ogni volta che vengono aperti dall'utente o dal computer	1. Aprire il riquadro di configurazione File e computer. In che modo? 1. Nel riquadro di sinistra, fare clic su **Menu avanzato**. 2. Fare clic su **Configura**. 3. Nel riquadro Configura, fare clic su **Computer e file**. 2. In **Protezione da virus**, fare clic su **Attiva**. **Nota**: la scansione in tempo reale è attivata per impostazione predefinita.
Avviare una scansione rapida per analizzare rapidamente il computer alla ricerca di minacce	1. Nel Menu standard, fare clic su **Esegui scansione**. 2. Nel riquadro Opzioni di scansione, in Scansione rapida, fare clic su **Avvia**.
Avviare una scansione completa per analizzare a fondo il computer alla ricerca di minacce	1. Nel Menu standard, fare clic su **Esegui scansione**. 2. Nel riquadro Opzioni di scansione, in Scansione completa, fare clic su **Avvia**.

Per...	Procedere come segue...
Avviare una scansione personalizzata in base alle proprie impostazioni	1. Nel Menu standard, fare clic su **Esegui scansione**. 2. Nel riquadro Opzioni di scansione, in Consenti scelta, fare clic su **Avvia**. 3. Personalizzare la scansione selezionando o deselezionando le seguenti opzioni: **Tutte le minacce in tutti i file** **Virus sconosciuti** **File di archivio** **Spyware e potenziali minacce** **Tracking cookie** **Programmi di mascheramento** 4. Fare clic su **Avvia**.
Avviare una scansione manuale per rilevare eventuali minacce in file, cartelle o unità	1. Aprire Esplora risorse. 2. Fare clic con il pulsante destro del mouse sul file, la cartella o l'unità, quindi scegliere **Esegui scansione**.

<table>
<tr><th>Per...</th><th>Procedere come segue...</th></tr>
<tr><td>Avviare una scansione pianificata per analizzare periodicamente il computer alla ricerca di minacce</td><td>1. Aprire il riquadro Scansione pianificata.
In che modo?
1. Nella sezione Attività comuni, fare clic su Home.
2. Nel riquadro SecurityCenter, fare clic su Computer e file.
3. Nell'area Computer e file, fare clic su Configura.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su Avanzate.
5. Fare clic su Scansione pianificata nel riquadro Protezione da virus.
2. Selezionare Attiva scansione pianificata.
3. Per ridurre la quantità di risorse del processore normalmente utilizzata per la scansione, selezionare Esegui scansione utilizzando risorse del computer minime.
4. Selezionare uno o più giorni.
5. Specificare un orario di inizio.
6. Fare clic su OK.</td></tr>
</table>

I risultati della scansione sono visualizzati nell'avviso di completamento della scansione. Nei risultati è incluso il numero di elementi sottoposti a scansione, rilevati, riparati, messi in quarantena e rimossi. Per ulteriori informazioni sui risultati della scansione o per gestire gli elementi infetti, fare clic su **Visualizza dettagli scansione**.

Nota: per maggiori informazioni sulle opzioni di scansione, vedere Tipi di scansione (pagina 40).

Come visualizzare i risultati della scansione

Al termine di una scansione, è possibile visualizzare i risultati per determinare gli elementi rilevati durante la scansione e analizzare lo stato attuale di protezione del computer. Nei risultati della scansione è possibile visualizzare se VirusScan ha rilevato, riparato o messo in quarantena virus, Trojan, spyware, adware, cookie e altri programmi potenzialmente indesiderati.

Nel menu standard o avanzato, fare clic su **Esegui scansione**, quindi eseguire una delle seguenti operazioni.

Per...	Procedere come segue...
Visualizzare i risultati della scansione nell'avviso	Visualizzare i risultati della scansione nell'avviso di completamento della scansione.
Visualizzare maggiori informazioni sui risultati della scansione	Fare clic su **Visualizza dettagli scansione** nell'avviso di completamento della scansione.
Visualizzare un riepilogo rapido dei risultati della scansione	Scegliere l'icona **Scansione completata** nell'area di notifica della barra delle applicazioni.
Visualizzare le statistiche di scansione e rilevamento	Fare doppio clic sull'icona **Scansione completata** nell'area di notifica della barra delle applicazioni.
Visualizzare i dettagli sugli elementi rilevati, lo stato e il tipo di infezione	1. Fare doppio clic sull'icona **Scansione completata** nell'area di notifica della barra delle applicazioni. 2. Fare clic su **Dettagli** nel riquadro Scansione completa, Scansione rapida, Scansione personalizzata o Scansione manuale.
Visualizzare i dettagli sulla scansione più recente	Fare doppio clic sull'icona **Scansione completata** nell'area di notifica della barra delle applicazioni e visualizzare i dettagli della scansione più recente in Analisi oppure nel riquadro Scansione completa, Scansione rapida, Scansione personalizzata o Scansione manuale.

CAPITOLO 10

Utilizzo dei risultati della scansione

Se VirusScan rileva una minaccia per la protezione durante l'esecuzione di una scansione, tenterà di gestirla automaticamente in base al tipo di minaccia. Se, ad esempio, VirusScan rileva un virus, Trojan o tracking cookie sul computer, tenta di pulire il file infetto. VirusScan mette sempre in quarantena un file prima di tentare di pulirlo. Se non è pulito, il file viene messo in quarantena.

Per alcune minacce alla protezione, VirusScan non riesce a pulire o mettere in quarantena un file. In questo caso, viene richiesto all'utente di gestire la minaccia. In base al tipo di minaccia è possibile adottare diverse azioni correttive. Se, ad esempio, viene rilevato un virus in un file, ma VirusScan non riesce a pulire o mettere in quarantena il file, l'accesso al file viene negato. Se vengono rilevati dei cookie, ma VirusScan non è in grado di pulirli o metterli in quarantena, l'utente può decidere se rimuoverli o considerarli affidabili. Se vengono rilevati programmi potenzialmente indesiderati, VirusScan non adotta alcuna azione automatica e l'utente può decidere di mettere in quarantena il programma o considerarlo affidabile.

Quando gli elementi vengono messi in quarantena, vengono crittografati e quindi isolati in una cartella per impedire ai file, programmi o cookie di danneggiare il computer. Gli elementi in quarantena possono essere ripristinati o rimossi. Nella maggior parte dei casi, è possibile eliminare un cookie in quarantena senza alcuna ripercussione sul sistema. Tuttavia, se VirusScan ha messo in quarantena un programma riconosciuto e utilizzato dall'utente, può essere opportuno ripristinarlo.

In questo capitolo

Come gestire virus e Trojan

Se VirusScan rileva un virus o un Trojan in un file sul computer, tenta di pulire il file. Se l'operazione di pulizia non riesce, cerca di metterlo in quarantena. Se anche questa operazione non riesce, l'accesso al file viene negato (solo scansioni in tempo reale).

1 Aprire il riquadro Risultati della scansione.

In che modo?

1. Fare doppio clic sull'icona **Scansione completata** nell'area di notifica a destra della barra delle applicazioni.
2. Nel riquadro Stato della scansione: Scansione manuale, fare clic su **Visualizza risultati**.

2 Nell'elenco dei risultati della scansione, fare clic su **Virus e Trojan**.

Nota: per utilizzare i file messi in quarantena da VirusScan, vedere Come utilizzare i file messi in quarantena (pagina 39).

Come utilizzare programmi potenzialmente indesiderati

Se VirusScan rileva un programma potenzialmente indesiderato sul computer, è possibile rimuovere il programma o considerarlo affidabile. Se non si conosce il programma, è consigliabile rimuoverlo. La rimozione del programma potenzialmente indesiderato non implica l'eliminazione effettiva dal sistema bensì la messa in quarantena, per impedire al programma di causare danni al computer o ai file.

1 Aprire il riquadro Risultati della scansione.

In che modo?

1. Fare doppio clic sull'icona **Scansione completata** nell'area di notifica a destra della barra delle applicazioni.
2. Nel riquadro Stato della scansione: Scansione manuale, fare clic su **Visualizza risultati**.

2 Nell'elenco dei risultati della scansione, fare clic su **Programmi potenzialmente indesiderati**.

3 Selezionare un programma potenzialmente indesiderato.

4 Nella sezione **Desidero**, fare clic su **Rimuovi** o **Considera affidabile**.

5 Confermare l'opzione selezionata.

Come utilizzare i file messi in quarantena

Quando i file infetti vengono messi in quarantena, sono crittografati e quindi spostati in una cartella per impedire ai file di danneggiare il computer. I file in quarantena possono quindi essere ripristinati o rimossi.

1 Aprire il riquadro File in quarantena.

In che modo?

1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
2. Fare clic su **Ripristina**.
3. Fare clic su **File**.

2 Selezionare un file in quarantena

3 Eseguire una delle seguenti operazioni:

- Per riparare il file infetto e ripristinarlo nel percorso originale sul computer, fare clic su **Ripristina**.
- Per rimuovere il file infetto dal computer, fare clic su **Rimuovi**.

4 Fare clic su **Sì** per confermare l'opzione selezionata.

Suggerimento: è possibile ripristinare o rimuovere più file contemporaneamente.

Come utilizzare i programmi e i cookie in quarantena

Quando i programmi potenzialmente indesiderati o i cookie traccianti vengono messi in quarantena, sono crittografati e quindi spostati in una cartella per impedire loro di danneggiare il computer. Gli elementi in quarantena possono quindi essere ripristinati o rimossi. Nella maggior parte dei casi, è possibile eliminare un elemento in quarantena senza alcuna ripercussione sul sistema.

1 Aprire il riquadro Programmi e cookie in quarantena.

In che modo?

1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
2. Fare clic su **Ripristina**.
3. Fare clic su **Programmi e cookie**.

2 Selezionare un programma o cookie in quarantena.

3 Eseguire una delle seguenti operazioni:
- Per riparare il file infetto e ripristinarlo nel percorso originale sul computer, fare clic su **Ripristina**.
- Per rimuovere il file infetto dal computer, fare clic su **Rimuovi**.

4 Fare clic su **Sì** per confermare l'operazione.

Suggerimento: è possibile ripristinare o rimuovere più programmi e cookie contemporaneamente.

Tipi di scansione

VirusScan offre una serie completa di opzioni di scansione per la protezione antivirus, inclusa la scansione in tempo reale, che monitora costantemente il computer per rilevare la presenza di eventuali attività di minaccia, la scansione manuale da Esplora risorse e la possibilità di eseguire una scansione completa, rapida o personalizzata da SecurityCenter o di personalizzare le eventuali scansioni pianificate. La scansione in SecurityCenter offre il vantaggio di modificare immediatamente le opzioni di scansione.

Scansione in tempo reale

La protezione antivirus in tempo reale controlla costantemente il computer per rilevare la presenza di eventuali attività di virus, analizzando i file ogni volta che vengono aperti dall'utente o dal computer. Per accertarsi che il computer resti protetto contro le minacce più recenti, attivare la protezione antivirus in tempo reale e pianificare scansioni manuali periodiche più complete.

È possibile impostare opzioni predefinite per la scansione in tempo reale, tra cui la scansione dei virus sconosciuti e il controllo delle eventuali minacce contenute nei cookie e nelle unità di rete. È inoltre possibile sfruttare la protezione da sovrascrittura del buffer, che è attivata per impostazione predefinita (tranne se si utilizza un sistema operativo Windows Vista a 64 bit). Per maggiori informazioni, vedere Impostazione delle opzioni di scansione in tempo reale (pagina 48).

Scansione rapida

La scansione rapida consente di controllare i processi, i file Windows di importanza fondamentale e altre aree vulnerabili sul computer al fine di rilevare la presenza di eventuali attività di minaccia.

Scansione completa

La scansione completa consente di esaminare minuziosamente l'intero computer per rilevare l'eventuale presenza di virus, spyware e altre minacce per la protezione sul PC.

Scansione personalizzata

La scansione personalizzata consente di configurare le impostazioni di scansione preferite per il controllo delle attività di minaccia sul PC. Le opzioni di scansione personalizzata comprendono il controllo delle minacce in tutti i file, nei file di archivio e nei cookie, oltre alla scansione di virus sconosciuti, spyware e programmi di mascheramento.

È possibile impostare opzioni predefinite per le scansioni personalizzate, tra cui la scansione di virus sconosciuti, file di archivio, spyware, minacce potenziali, tracking cookie e programmi di mascheramento. È anche possibile eseguire la scansione utilizzando risorse del computer minime. Per maggiori informazioni, vedere Impostazione delle opzioni di scansione personalizzata (pagina 51).

Scansione manuale

La scansione manuale consente di controllare rapidamente l'eventuale presenza di minacce in file, cartelle e unità da Esplora risorse.

Scansione pianificata

Le scansioni pianificate eseguono una ricerca accurata dei virus e di altre minacce nel computer in qualsiasi giorno e ora della settimana. Le scansioni pianificate consentono di controllare l'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana. Se si riscontrano problemi di lentezza della scansione, si consideri la disattivazione dell'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività. Per maggiori informazioni, vedere Pianificazione di una scansione (pagina 54).

Nota: per istruzioni su come avviare l'opzione di scansione più adeguata alle proprie esigenze, vedere Come analizzare il PC (pagina 32).

CAPITOLO 11

Utilizzo di ulteriori protezioni

In aggiunta alla protezione da virus in tempo reale, VirusScan offre la protezione avanzata da script, spyware e allegati di posta elettronica e di messaggistica immediata potenzialmente dannosi. Per impostazione predefinita, la protezione con scansione script, spyware, posta elettronica e messaggistica immediata è attiva e in funzione.

Protezione con scansione script

La scansione script rileva gli script potenzialmente dannosi e ne impedisce l'esecuzione sul computer o nel browser Web. Controlla eventuali attività sospette del computer, ad esempio uno script che crea, copia o elimina dei file oppure apre il registro di sistema di Windows, avvisando l'utente prima che si verifichi qualsiasi danno.

Protezione da spyware

La protezione da spyware rileva eventuale spyware, adware e altri programmi potenzialmente indesiderati. Lo spyware è un software che può essere segretamente installato sul computer per controllare il comportamento dell'utente, raccogliere dati personali e interferire persino con il controllo del computer da parte dell'utente, installando software aggiuntivo oppure reindirizzando l'attività del browser.

Protezione della posta elettronica

La protezione della posta elettronica rileva le attività sospette nei messaggi e negli allegati di posta elettronica inviati.

Protezione della messaggistica immediata

La protezione della messaggistica immediata consente di rilevare le potenziali minacce per la sicurezza contenute negli allegati ai messaggi immediati ricevuti. Impedisce inoltre la condivisione di dati personali nei programmi di messaggistica immediata.

In questo capitolo

Avviare la protezione con scansione script

Attivare la scansione script per rilevare gli script potenzialmente dannosi e impedirne l'esecuzione sul computer. La scansione script avvisa quando uno script tenta di creare, copiare o eliminare dei file sul computer oppure di apportare modifiche al registro di sistema di Windows.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione con scansione script**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione con scansione script in qualsiasi momento, in tal modo si renderà il computer vulnerabile agli script dannosi.

Come avviare la protezione antispyware

Attivare la protezione da spyware per rilevare e rimuovere spyware, adware e altri programmi potenzialmente indesiderati che raccolgono e trasmettono informazioni senza l'autorizzazione dell'utente o a sua insaputa.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione con scansione script**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione da spyware in qualsiasi momento, in tal modo si renderà il computer vulnerabile ai programmi potenzialmente indesiderati.

Come avviare la protezione della posta elettronica

Attivare la protezione della posta elettronica per rilevare worm e le potenziali minacce contenute nei messaggi di posta elettronica in uscita (SMTP) e in arrivo (POP3), nonché negli allegati.

1 Aprire il riquadro di configurazione Posta elettronica e MI.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.

2 In **Protezione della posta elettronica**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione della posta elettronica in qualsiasi momento, in tal modo si renderà il computer vulnerabile alle minacce della posta elettronica.

Come avviare la protezione della messaggistica immediata

Attivare la protezione della messaggistica immediata per rilevare le minacce per la sicurezza che possono essere contenute negli allegati ai messaggi immediati in arrivo.

1 Aprire il riquadro di configurazione Posta elettronica e MI.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.

2 In **Protezione messaggistica immediata**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione della messaggistica immediata in qualsiasi momento, in tal modo si renderà il computer vulnerabile agli allegati dei messaggi immediati.

CAPITOLO 12

Impostazione della protezione da virus

È possibile impostare diverse opzioni per la scansione pianificata, personalizzata e in tempo reale. Ad esempio, poiché la protezione in tempo reale controlla ininterrottamente il computer, è possibile selezionare una determinata serie di opzioni di scansione di base, riservando una serie di opzioni di scansione più completa alla protezione manuale su richiesta.

È anche possibile decidere in che modo VirusScan eseguirà il controllo e la gestione delle modifiche potenzialmente non autorizzate o indesiderate sul PC utilizzando i moduli SystemGuard e gli elenchi di elementi affidabili. I moduli SystemGuard controllano, registrano, segnalano e gestiscono le modifiche potenzialmente non autorizzate apportate al registro di sistema di Windows oppure ai file di sistema importanti sul computer. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti. È possibile utilizzare il riquadro Elementi affidabili per impostare come affidabili o rimuovere le regole di rilevamento delle modifiche apportate a file o al registro di sistema (SystemGuard), programmi o sovraccarichi del buffer. Se l'utente imposta l'elemento come affidabile e richiede di non ricevere notifiche future sulla relativa attività, l'elemento viene aggiunto a un elenco di elementi affidabili e VirusScan non rileva più o non invia più notifiche all'utente in merito all'attività di tale elemento.

In questo capitolo

Impostazione delle opzioni di scansione in tempo reale

Quando l'utente avvia la protezione antivirus in tempo reale, VirusScan utilizza una serie predefinita di opzioni per la scansione dei file. È tuttavia possibile modificare le opzioni predefinite in base alle proprie esigenze.

Per modificare le opzioni di scansione in tempo reale, è necessario decidere quali elementi saranno controllati da VirusScan durante una scansione, nonché i percorsi e i tipi di file sottoposti a scansione. Ad esempio, è possibile determinare se VirusScan deve controllare virus o cookie sconosciuti, che i siti Web possono utilizzare per tenere traccia del comportamento dell'utente, e se deve sottoporre a scansione le unità di rete mappate al computer in uso o semplicemente le unità locali. L'utente può inoltre determinare quali tipi di file vengono sottoposti a scansione (tutti i file oppure solo i file di programma e i documenti, in cui viene rilevata la maggior parte dei virus).

Quando si modificano le opzioni di scansione in tempo reale è inoltre necessario stabilire l'importanza della protezione dal sovraccarico del buffer sul computer in uso. Un buffer è una parte di memoria utilizzata per contenere temporaneamente informazioni sul computer. I sovraccarichi del buffer possono verificarsi quando la quantità di informazioni memorizzate nel buffer da programmi o processi sospetti supera la capacità dello stesso. In questo caso, il computer diviene vulnerabile agli attacchi.

Come impostare le opzioni di scansione in tempo reale

L'utente può impostare le opzioni di scansione in tempo reale in modo da personalizzare gli elementi controllati da VirusScan durante una scansione in tempo reale, nonché i percorsi e i tipi di file sottoposti a scansione. Tra le opzioni disponibili è inclusa la scansione di virus sconosciuti e tracking cookie, nonché la protezione dal sovraccarico del buffer. È inoltre possibile configurare la scansione in tempo reale per controllare le unità di rete mappate al computer in uso.

1 Aprire il riquadro Scansione in tempo reale.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.

2 Specificare le opzioni di scansione in tempo reale desiderate, quindi fare clic su **OK**.

Per...	Procedere come segue...
Rilevare virus sconosciuti e nuove varianti di virus noti	Selezionare **Cerca virus sconosciuti**.
Rilevare i cookie	Selezionare **Cerca e rimuovi cookie**.
Rilevare virus e altre minacce potenziali sulle unità connesse alla rete	Selezionare **Esegui scansione su unità di rete**.
Proteggere il computer contro i sovraccarichi del buffer	Selezionare **Attiva protezione dal sovraccarico del buffer**.
Specificare i tipi di file da analizzare	Fare clic su **Tutti i file (consigliato)** o **Solo file di programma e documenti**.

Come interrompere la protezione antivirus in tempo reale

In rari casi, potrebbe essere opportuno sospendere temporaneamente la scansione in tempo reale (ad esempio, per modificare alcune opzioni di scansione oppure per risolvere problemi legati alle prestazioni). Se la protezione antivirus in tempo reale è disattivata, il computer non è protetto e lo stato di protezione di SecurityCenter è rosso. Per ulteriori informazioni sullo stato di protezione, vedere "Informazioni sullo stato della protezione" nella guida di SecurityCenter.

È possibile disattivare temporaneamente la protezione da virus in tempo reale, quindi specificare l'orario di ripristino. La protezione può essere ripristinata automaticamente dopo un intervallo di 15, 30, 45 o 60 minuti, al riavvio del computer oppure mai.

1 Aprire il riquadro di configurazione File e computer.

   In che modo?

   1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
   2. Fare clic su **Configura**.
   3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione da virus**, fare clic su **Disattiva**.

3 Nella finestra di dialogo, scegliere quando ripristinare la scansione in tempo reale.

4 Fare clic su **OK**.

Impostazione delle opzioni di scansione personalizzata

La protezione antivirus personalizzata consente di eseguire la scansione dei file su richiesta. Quando si avvia una scansione personalizzata, VirusScan rileva l'eventuale presenza di virus e di altri elementi potenzialmente dannosi sul computer, utilizzando una gamma più completa di opzioni di scansione. Per modificare le opzioni di scansione personalizzata, è necessario decidere quali elementi saranno controllati da VirusScan durante una scansione. Ad esempio, è possibile configurare la ricerca e l'analisi di virus sconosciuti, di programmi potenzialmente indesiderati, come spyware o adware, di programmi di mascheramento e rootkit, che possono concedere l'accesso non autorizzato al computer, e dei cookie, che vengono utilizzati dai siti Web per tenere traccia del comportamento dell'utente. L'utente può inoltre stabilire il tipo di file su cui eseguire il controllo. Ad esempio, è possibile determinare se VirusScan deve controllare tutti i file oppure solo i file di programma e i documenti, in cui viene rilevata la maggior parte dei virus. È inoltre possibile stabilire se includere i file di archivio (ad esempio, i file .zip) nella scansione.

Per impostazione predefinita, VirusScan controlla tutte le unità e le cartelle sul computer in uso e su tutte le unità di rete ogni volta che viene eseguita una scansione personalizzata. Tuttavia, è possibile modificare i percorsi predefiniti in base alle proprie esigenze. Ad esempio, è possibile eseguire la scansione solo di file di importanza critica, degli elementi presenti sul desktop oppure di quelli contenuti nella cartella Programmi. Se l'utente non desidera essere responsabile dell'avvio di ogni scansione personalizzata, è possibile impostare una pianificazione periodica delle scansioni. Le scansioni pianificate consentono di controllare l'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana.

Se si riscontrano problemi di lentezza della scansione, si consideri la disattivazione dell'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività.

Nota: quando sul computer si riproducono film, videogiochi o si eseguono altre applicazioni che occupano l'intero schermo, VirusScan sospende alcune attività, tra cui gli aggiornamenti automatici e le scansioni personalizzate.

Come impostare le opzioni di scansione personalizzata

L'utente può impostare le opzioni di scansione personalizzata in modo da personalizzare gli elementi controllati da VirusScan durante una scansione personalizzata, nonché i percorsi e i tipi di file sottoposti a scansione. Tra le opzioni disponibili è inclusa la scansione di virus sconosciuti, archivi di file, spyware e programmi potenzialmente indesiderati, cookie, rootkit e programmi di mascheramento. È inoltre possibile impostare il percorso di scansione personalizzata in cui VirusScan dovrà rilevare l'eventuale presenza di virus e altri elementi dannosi. È possibile analizzare tutti i file, le cartelle e le unità del computer oppure limitare la scansione a cartelle e unità specifiche.

1 Aprire il riquadro Scansione personalizzata.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Fare clic su **Scansione manuale** nel riquadro Protezione da virus.

2 Specificare le opzioni di scansione personalizzata desiderate, quindi fare clic su **OK**.

Per...	Procedere come segue...
Rilevare virus sconosciuti e nuove varianti di virus noti	Selezionare **Cerca virus sconosciuti**.
Rilevare e rimuovere i virus nei file .zip e in altri file di archivio	Selezionare **Analizza file di archivio**.
Rilevare spyware, adware e altri programmi potenzialmente indesiderati	Selezionare **Cerca spyware e potenziali minacce**.
Rilevare i cookie	Selezionare **Cerca e rimuovi cookie**.
Rilevare rootkit e programmi di mascheramento che possono modificare e sfruttare i file di sistema di Windows esistenti	Selezionare **Cerca programmi mascherati**.

Per...	Procedere come segue...
Utilizzare una quantità minore di risorse del processore per le scansioni, assegnando maggiore priorità ad altre attività (quali la navigazione su Internet o l'apertura di documenti)	Selezionare **Esegui scansione utilizzando risorse del computer minime**.
Specificare i tipi di file da analizzare	Fare clic su **Tutti i file (consigliato)** o **Solo file di programma e documenti**.

3 Fare clic su **Percorso predefinito da sottoporre a scansione**, quindi selezionare o deselezionare i percorsi che si desidera analizzare o ignorare, infine fare clic su **OK**:

Per...	Procedere come segue...
Analizzare tutti i file e le cartelle sul computer	Selezionare **Risorse del computer**.
Analizzare file, cartelle e unità specifiche sul computer	Deselezionare la casella di controllo **Risorse del computer** e selezionare una o più cartelle o unità.
Analizzare i file di sistema critici	Deselezionare la casella di controllo **Risorse del computer**, quindi selezionare la casella di controllo **File di sistema importanti**.

Pianificazione di una scansione

È possibile pianificare le scansioni per una ricerca accurata dei virus e di altre minacce nel computer in qualsiasi giorno e ora della settimana. Le scansioni pianificate consentono di controllare l'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana. Se si riscontrano problemi di lentezza della scansione, si consideri la disattivazione dell'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività.

È possibile pianificare le scansioni per una ricerca accurata dei virus e di altre minacce nell'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana.

1 Aprire il riquadro Scansione pianificata.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
   3. Nell'area Computer e file, fare clic su **Configura**.
   4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
   5. Fare clic su **Scansione pianificata** nel riquadro Protezione da virus.

2 Selezionare **Attiva scansione pianificata**.

3 Per ridurre la quantità di risorse del processore normalmente utilizzata per la scansione, selezionare **Esegui scansione utilizzando risorse del computer minime**.

4 Selezionare uno o più giorni.

5 Specificare un orario di inizio.

6 Fare clic su **OK**.

Suggerimento: è possibile ripristinare la pianificazione predefinita facendo clic su **Ripristina**.

Utilizzo delle opzioni SystemGuard

I moduli SystemGuard controllano, registrano, segnalano e gestiscono le modifiche potenzialmente non autorizzate apportate al registro di sistema di Windows oppure ai file di sistema importanti sul computer. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

Le modifiche del registro di sistema e dei file sono comuni e si verificano periodicamente sul computer. Poiché molte di esse sono innocue, le impostazioni predefinite dei moduli SystemGuard sono configurate in modo da offrire una protezione affidabile, intelligente e reale contro le modifiche non autorizzate e potenzialmente dannose. Ad esempio, quando i moduli SystemGuard rilevano modifiche non comuni che rappresentano una minaccia potenzialmente significativa, tali attività vengono immediatamente segnalate e registrate. Le modifiche comuni, ma comunque potenzialmente dannose, vengono solamente registrate. Il controllo delle modifiche standard o a basso rischio è comunque disattivato per impostazione predefinita. È possibile configurare la tecnologia SystemGuard in modo da estenderne la protezione a qualsiasi ambiente desiderato.

Esistono tre tipi di SystemGuard: SystemGuard programmi, SystemGuard Windows e SystemGuard browser.

SystemGuard programmi

Il modulo SystemGuard programmi rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Tra questi importanti elementi del registro di sistema e file sono incluse le installazioni di ActiveX, gli elementi del menu di avvio, gli hook di esecuzione della shell di Windows e le chiavi ShellServiceObjectDelayLoad. Monitorando tali file, la tecnologia SystemGuard programmi arresta i programmi ActiveX (scaricati da Internet) nonché i programmi spyware e potenzialmente indesiderati che possono essere automaticamente eseguiti all'avvio di Windows.

SystemGuard Windows

Anche il modulo SystemGuard Windows rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Tra questi importanti elementi del registro di sistema e file sono inclusi i gestori dei menu, i file DLL appInit e i file host di Windows. Monitorando questi file, la tecnologia SystemGuard Windows contribuisce a prevenire l'invio e la ricezione di informazioni non autorizzate o personali dal computer a Internet. Consente inoltre di arrestare programmi sospetti che possono apportare modifiche non desiderate all'aspetto e al funzionamento di programmi importanti per l'utente e i suoi familiari.

SystemGuard browser

Come i moduli SystemGuard programmi e SystemGuard Windows, anche il modulo SystemGuard browser rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. SystemGuard browser, tuttavia, controlla le modifiche apportate a elementi del registro di sistema e file, come i componenti aggiuntivi, gli URL e le aree di protezione di Internet Explorer. Monitorando questi file, la tecnologia SystemGuard browser contribuisce a prevenire le attività del browser non autorizzate, come il reindirizzamento a siti Web sospetti, le modifiche apportate alle impostazioni e alle opzioni del browser all'insaputa dell'utente e l'impostazione non desiderata di siti Web sospetti come affidabili.

Come attivare la protezione SystemGuard

Attivare la protezione SystemGuards per rilevare e avvisare l'utente delle modifiche potenzialmente non autorizzate apportate al registro di sistema di Windows e ai file sul computer in uso. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione SystemGuard**, fare clic su **Attiva**.

Nota: è possibile disattivare la protezione SystemGuard facendo clic su **Disattiva**.

Come configurare le opzioni SystemGuard

Utilizzare il riquadro SystemGuard per configurare le opzioni di protezione, registrazione e avviso contro modifiche non autorizzate del registro di sistema e dei file, associate a file e programmi di Windows nonché a Internet Explorer. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

1 Aprire il riquadro SystemGuard.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione SystemGuard sia attivata, quindi fare clic su **Avanzate**.

2 Selezionare un tipo di SystemGuard dall'elenco.

- **SystemGuard programmi**
- **SystemGuard Windows**
- **SystemGuard browser**

3 In **Desidero**, effettuare una delle seguenti operazioni:

- Per rilevare, registrare e segnalare modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Mostra avvisi**.
- Per rilevare e registrare modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Registra solo le modifiche**.
- Per disattivare il rilevamento delle modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Disattiva SystemGuard**.

Nota: per ulteriori informazioni sui tipi di SystemGuard, vedere Informazioni sui tipi di SystemGuard (pagina 58).

Informazioni sui tipi di SystemGuard

I moduli SystemGuard rilevano le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Esistono tre tipi di SystemGuard: SystemGuard programmi, SystemGuard Windows e SystemGuard browser.

SystemGuard programmi

La tecnologia SystemGuard programmi blocca i programmi ActiveX sospetti (scaricati da Internet), nonché i programmi spyware e potenzialmente indesiderati in grado di avviarsi automaticamente all'avvio di Windows.

SystemGuard	Rileva...
Installazioni di ActiveX	Modifiche non autorizzate al registro di sistema per le installazioni di ActiveX che possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.
Elementi di avvio	Programmi spyware, adware o potenzialmente indesiderati che possono apportare modifiche ai file per gli elementi di avvio, consentendo l'esecuzione di programmi sospetti all'avvio del computer.
Hook di esecuzione della shell di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di installare gli hook di esecuzione della shell di Windows per impedire la corretta esecuzione dei programmi di protezione.
Chiave ShellServiceObjectDelayLoad	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche alla chiave ShellServiceObjectDelayLoad del registro di sistema, consentendo l'esecuzione di file pericolosi all'avvio del computer.

SystemGuard Windows

La tecnologia SystemGuard Windows consente di impedire al computer l'invio e la ricezione di informazioni non autorizzate o personali su Internet. Consente inoltre di bloccare programmi sospetti che possono apportare modifiche non desiderate all'aspetto e al funzionamento di programmi importanti per l'utente e i suoi familiari.

SystemGuard	Rileva...
Gestori dei menu di scelta rapida	Modifiche non autorizzate al registro di sistema per i gestori dei menu di scelta rapida di Windows che possono incidere sull'aspetto e sul comportamento dei menu di Windows. I menu di scelta rapida consentono di eseguire azioni sul computer, ad esempio fare clic sui file con il pulsante destro del mouse.
DLL AppInit	Modifiche non autorizzate alle DDL appInit del registro di sistema di Windows in grado di consentire l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
File hosts di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche non autorizzate al file hosts di Windows, consentendo il reindirizzamento del browser a siti Web sospetti e il blocco degli aggiornamenti del software.
Shell di Winlogon	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per la shell di Winlogon, consentendo la sostituzione di Esplora risorse di Windows con altri programmi.
Chiave UserInit di Winlogon	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche alla chiave UserInit di Winlogon del registro di sistema, consentendo l'esecuzione di programmi sospetti quando l'utente esegue l'accesso a Windows.
Protocolli Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i protocolli Windows che si riflettono sulle modalità di invio e ricezione di informazioni su Internet del computer.
Layered Service Provider di Winsock	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli LSP (Layered Service Provider) di Winsock, al fine di intercettare e modificare le informazioni inviate e ricevute su Internet.

SystemGuard	Rileva...
Comandi Apri della shell di Windows	Modifiche non autorizzate ai comandi Apri della shell di Windows che possono determinare l'esecuzione di worm e di altri programmi potenzialmente pericolosi sul computer.
Utilità di pianificazione condivisa	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema e ai file per l'Utilità di pianificazione condivisa, consentendo l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
Windows Messenger Service	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per Windows Messenger Service, consentendo la visualizzazione di pubblicità non richiesta e l'esecuzione in modalità remota di programmi sul computer.
File Win.ini di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al file Win.ini, consentendo l'esecuzione di programmi sospetti all'avvio del computer.

SystemGuard browser

La tecnologia SystemGuard browser consente di impedire attività del browser non autorizzate, come il reindirizzamento a siti Web sospetti, le modifiche apportate a impostazioni e opzioni del browser all'insaputa dell'utente e l'impostazione indesiderata di siti Web sospetti come affidabili.

SystemGuard	Rileva...
Oggetti helper browser	Programmi spyware, adware o potenzialmente indesiderati in grado di utilizzare gli oggetti helper del browser per tenere traccia delle abitudini di navigazione sul Web dell'utente e visualizzare pubblicità non richiesta.
Barre di Internet Explorer	Modifiche non autorizzate al registro di sistema per le barre di Internet Explorer, ad esempio Cerca e Preferiti, che possono incidere sull'aspetto e sul comportamento di Internet Explorer.
Componenti aggiuntivi di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di installare componenti aggiuntivi di Internet Explorer per tenere traccia delle abitudini di navigazione sul Web dell'utente e visualizzare pubblicità non richiesta.

SystemGuard	Rileva...
ShellBrowser di Internet Explorer	Modifiche non autorizzate al registro di sistema per il componente ShellBrowser di Internet Explorer che possono incidere sull'aspetto e sul comportamento del browser Web in uso.
WebBrowser di Internet Explorer	Modifiche non autorizzate al registro di sistema per il componente WebBrowser di Internet Explorer che possono incidere sull'aspetto e sul comportamento del browser in uso.
Hook di ricerca URL di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli hook di ricerca degli URL di Internet Explorer, consentendo il reindirizzamento del browser a siti Web sospetti durante le ricerche su Internet.
URL di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli URL di Internet Explorer che si riflettono sulle impostazioni del browser.
Restrizioni di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per le restrizioni di Internet Explorer che si riflettono sulle impostazioni e sulle opzioni del browser.
Aree di protezione di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per le aree di protezione di Internet Explorer, consentendo l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
Siti attendibili di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i siti attendibili di Internet Explorer, consentendo al browser di considerare affidabili siti Web sospetti.
Criterio di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i criteri di Internet Explorer che si riflettono sulle impostazioni e sul comportamento del browser.

Utilizzo degli elenchi di elementi affidabili

Se VirusScan rileva una modifica al registro di sistema o ai file (SystemGuard), un programma o un sovraccarico del buffer, avvisa l'utente di impostarlo come affidabile o rimuoverlo. Se l'utente imposta l'elemento come affidabile e richiede di non ricevere notifiche future sulla relativa attività, l'elemento viene aggiunto a un elenco di elementi affidabili e VirusScan non rileva più o non invia più notifiche all'utente in merito all'attività di tale elemento. Se un elemento è stato aggiunto a un elenco di elementi affidabili, l'utente può comunque decidere di bloccarne l'attività. Il blocco impedisce all'elemento di essere eseguito o di apportare modifiche al computer senza informare l'utente ogni volta che viene fatto un tentativo. L'elemento può anche essere rimosso dall'elenco di elementi affidabili. Quando si rimuove l'elemento, VirusScan è in grado di rilevarne nuovamente l'attività.

Come gestire gli elenchi di elementi affidabili

Utilizzare il riquadro Elementi affidabili per impostare come affidabili o bloccare gli elementi precedentemente rilevati e considerati affidabili. È inoltre possibile rimuovere un elemento dall'elenco di elementi affidabili in modo da consentirne il rilevamento da parte di VirusScan.

1 Aprire il riquadro Elementi affidabili.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Nel riquadro Protezione da virus, fare clic su **Elementi affidabili**.

2 Selezionare uno dei seguenti tipi di elementi affidabili:

- **SystemGuard programmi**
- **SystemGuard Windows**
- **SystemGuard browser**
- **Programmi affidabili**
- **Sovraccarichi del buffer affidabili**

3 In **Desidero**, effettuare una delle seguenti operazioni:

- Per consentire all'elemento rilevato di apportare modifiche al registro di sistema di Windows o a file di sistema critici sul computer senza informare l'utente, fare clic su **Affidabile**.
- Per impedire all'elemento rilevato di apportare modifiche al registro di sistema di Windows o a file di sistema critici sul computer senza informare l'utente, fare clic su **Blocca**.
- Per rimuovere l'elemento rilevato dall'elenco di elementi affidabili, fare clic su **Rimuovi**.

4 Fare clic su **OK**.

Nota: per ulteriori informazioni sui tipi di elementi affidabili, vedere Informazioni sui tipi di elementi affidabili (pagina 63).

Informazioni sui tipi di elementi affidabili

I SystemGuard del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. Vi sono cinque tipi di elementi affidabili che è possibile gestire dal riquadro Elementi affidabili: SystemGuard programmi, SystemGuard Windows, SystemGuard browser, programmi affidabili e sovraccarichi del buffer affidabili.

Opzione	Descrizione
SystemGuard programmi	I SystemGuard programmi del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard programmi rilevano le modifiche non autorizzate al registro di sistema e ai file associate alle installazioni ActiveX, agli elementi di avvio, agli hook di esecuzione della shell di Windows e all'attività ShellServiceObjectDelayLoad. Tali tipi di modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

Opzione	Descrizione
SystemGuard Windows	I SystemGuard Windows del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard Window rilevano modifiche non autorizzate al registro di sistema e ai file associate ai gestori dei menu di scelta rapida, ai DLL appInit, al file hosts di Windows, alla shell di Winlogon, agli LSP (Layered Service Provider) di Winsock e così via. Tali tipi di modifiche non autorizzate al registro di sistema e ai file possono ripercuotersi sulle modalità di invio e ricezione delle informazioni su Internet da parte del computer, modificare l'aspetto e il comportamento dei programmi e consentire l'esecuzione di programmi sospetti sul computer.
SystemGuard browser	I SystemGuard browser del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard browser rilevano modifiche non autorizzate al registro di sistema o altro comportamento indesiderato associato agli oggetti helper del browser, ai componenti aggiuntivi di Internet Explorer, agli URL di Internet Explorer, alle aree di protezione di Internet Explorer e così via. Tali tipi di modifiche non autorizzate al registro possono indurre attività del browser indesiderate come il reindirizzamento a siti Web sospetti, la modifica di impostazioni e opzioni del browser e l'impostazione involontaria di siti Web sospetti come siti affidabili.
Programmi affidabili	I programmi affidabili sono programmi potenzialmente indesiderati rilevati da VirusScan che l'utente ha deciso di considerare come affidabili da un avviso o dal riquadro Risultati della scansione.
Sovraccarichi del buffer affidabili	I sovraccarichi del buffer affidabili rappresentano attività precedentemente indesiderate rilevate da VirusScan ma che l'utente ha deciso di considerare come affidabili da un avviso o dal riquadro Risultati della scansione. I sovraccarichi del buffer possono nuocere al computer e danneggiare i file. I sovraccarichi del buffer si verificano quando la quantità di informazioni memorizzate nel buffer da programmi o processi sospetti supera la capacità dello stesso.

CAPITOLO 13

McAfee Personal Firewall

Personal Firewall offre una protezione avanzata per il computer e per i dati personali. Personal Firewall consente di stabilire una barriera tra il computer in uso e Internet, monitorando il traffico Internet alla ricerca di attività sospette, senza richiedere interazione da parte dell'utente.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Personal Firewall

Livelli di protezione standard e personalizzati	Protezione contro le intrusioni e le attività sospette mediante le impostazioni di protezione predefinite o personalizzabili del firewall.
Consigli in tempo reale	Il firewall offre l'opportunità di ricevere in maniera dinamica alcuni consigli che aiutano a decidere a quali programmi consentire l'accesso a Internet e se ritenere affidabile il traffico di rete.
Gestione intelligente dell'accesso per i programmi	Gestione dell'accesso a Internet per i programmi, mediante avvisi e registri degli eventi, e configurazione delle autorizzazioni di accesso per programmi specifici.
Protezione durante l'esecuzione di giochi	È possibile impedire la visualizzazione di avvisi relativi a tentativi di intrusione e attività sospette che possono distrarre l'utente durante l'esecuzione di giochi a schermo intero.
Protezione all'avvio del computer	Protegge il computer da tentativi di intrusione, programmi e traffico di rete indesiderati all'avvio di Windows®.
Controllo delle porte dei servizi di sistema	Gestione delle porte dei servizi di sistema aperte e chiuse necessarie per alcuni programmi.
Gestione delle connessioni del computer	È possibile consentire e bloccare le connessioni tra il proprio computer e altri computer.
Integrazione delle informazioni di HackerWatch	Rilevamento di sequenze generali di attività di hacker e intrusioni attraverso il sito Web di HackerWatch, che inoltre fornisce dati aggiornati sulla protezione in relazione ai programmi presenti sul computer, nonché statistiche globali sugli eventi di protezione e sulle porte Internet.
Blocca firewall	Consente di bloccare immediatamente tutto il traffico in ingresso e in uscita tra il computer e Internet.
Ripristina firewall	Ripristina immediatamente le impostazioni di protezione originali del firewall.
Rilevamento avanzato di Trojan	Consente di rilevare e bloccare applicazioni potenzialmente dannose, come i Trojan, che potrebbero diffondere i dati personali dell'utente su Internet.
Registrazione eventi	Tiene traccia degli eventi in ingresso, in uscita e di intrusione più recenti.
Monitoraggio del traffico Internet	Analisi delle mappe che illustrano l'origine degli attacchi dannosi e del traffico a livello mondiale. Inoltre, è possibile individuare informazioni dettagliate sui proprietari e dati geografici relativi agli indirizzi IP di origine. Il firewall consente inoltre di analizzare il traffico in ingresso e in uscita, monitorare l'utilizzo della larghezza di banda dei programmi e le attività dei programmi.
Prevenzione delle intrusioni	Aumenta la protezione della privacy contro possibili minacce Internet. Mediante una funzionalità di tipo euristico, viene offerto un terzo livello di protezione bloccando gli elementi che presentano i sintomi di un attacco o le caratteristiche di un tentativo di intrusione.

Analisi complessa del traffico

Consente di analizzare il traffico Internet in ingresso e in uscita, nonché le connessioni dei programmi, compresi quelli attivamente in ascolto di connessioni aperte. In questo modo è possibile rilevare i programmi vulnerabili a un'eventuale intrusione e intervenire di conseguenza.

CAPITOLO 14

Avvio del firewall

Una volta installato il firewall, il computer è protetto da intrusioni e da traffico di rete indesiderato. Inoltre l'utente è pronto a gestire gli avvisi e l'accesso Internet in ingresso e in uscita di programmi noti e sconosciuti. Sono automaticamente selezionati i suggerimenti intelligenti e il livello di protezione Automatica (con l'opzione che consente per i programmi l'accesso a Internet solo in uscita).

È anche possibile disattivare il firewall dal riquadro Configurazione di Internet e rete ma, in questo caso, il computer non sarà più protetto da intrusioni e da traffico di rete indesiderato e l'utente non potrà gestire in maniera efficace le connessioni Internet in ingresso e in uscita. Pertanto, la protezione firewall deve essere disattivata solo temporaneamente e in caso di necessità. Il firewall può essere anche attivato dal pannello Configurazione di Internet e rete.

Il firewall disattiva automaticamente Windows® Firewall e imposta se stesso come firewall predefinito.

Nota: per configurare Personal Firewall, aprire il riquadro Configurazione di Internet e rete.

In questo capitolo

Avvio della protezione firewall

È possibile attivare il firewall per proteggere il computer dalle intrusioni e dal traffico di rete indesiderato, nonché per gestire le connessioni Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è disattivata**, fare clic su **Attiva**.

Come arrestare la protezione firewall

È possibile disattivare il firewall se non si desidera proteggere il computer dalle intrusioni e dal traffico di rete indesiderato. Se il firewall è disattivato, non è possibile gestire le connessioni Internet in ingresso o in uscita.

1 Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.

2 Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Disattiva**.

CAPITOLO 15

Utilizzo degli avvisi

Il firewall utilizza una serie di avvisi che facilitano la gestione della protezione da parte dell'utente. Questi avvisi possono essere raggruppati in tre tipi principali:

- Avviso rosso
- Avviso giallo
- Avviso verde

Gli avvisi possono anche contenere informazioni utili per decidere come gestire gli avvisi o ottenere informazioni sui programmi in esecuzione sul computer.

In questo capitolo

Informazioni sugli avvisi

Il firewall prevede tre tipi principali di avvisi. Alcuni avvisi, inoltre, includono informazioni utili all'apprendimento o al reperimento di informazioni relative ai programmi in esecuzione sul computer.

Avviso rosso

L'avviso rosso viene visualizzato quando il firewall rileva, e quindi blocca, un Trojan sul computer e suggerisce una scansione per la ricerca di altre minacce. Un Trojan ha l'aspetto di un programma legittimo, ma può consentire l'accesso non autorizzato al computer, provocarne malfunzionamenti e danneggiarlo. Questo tipo di avviso può verificarsi su tutti i livelli di protezione.

Avviso giallo

Il tipo più comune di avviso è quello giallo, che informa l'utente quando il firewall rileva un'attività di programma o un evento di rete. In questi casi, l'avviso descrive l'attività di programma o evento di rete e fornisce una o più opzioni che richiedono una risposta da parte dell'utente. Ad esempio, l'avviso **Nuova connessione di rete** viene visualizzato quando un computer su cui è installato il firewall è connesso a una nuova rete. È possibile specificare il livello di affidabilità che si desidera assegnare alla nuova rete, che verrà quindi visualizzato nell'elenco delle reti. Se sono attivati i suggerimenti intelligenti, i programmi noti vengono aggiunti automaticamente al riquadro Autorizzazioni programmi.

Avviso verde

Nella maggior parte dei casi, un avviso verde fornisce informazioni di base su un evento, senza richiedere alcuna risposta da parte dell'utente. Gli avvisi verdi sono disattivati per impostazione predefinita.

Assistenza per l'utente

Molti avvisi firewall contengono ulteriori informazioni che consentono di gestire con facilità la protezione del computer, tra cui:

- **Ulteriori informazioni su questo programma**: viene avviato il sito Web di protezione globale di McAfee che fornisce informazioni su un programma che il firewall ha rilevato sul computer.
- **Informa McAfee di questo programma**: vengono inviate informazioni a McAfee su un file sconosciuto rilevato sul computer dal firewall.
- **McAfee suggerisce**: vengono forniti suggerimenti per la gestione degli avvisi. Ad esempio, un avviso può suggerire di concedere l'accesso a un programma.

CAPITOLO 16

Gestione degli avvisi informativi

Il firewall consente di visualizzare o nascondere gli avvisi informativi quando rileva un tentativo di intrusione o un'attività sospetta nel corso di determinati eventi, ad esempio durante l'esecuzione di giochi a schermo intero.

In questo capitolo

Visualizzazione degli avvisi durante l'esecuzione di giochi

È possibile consentire la visualizzazione degli avvisi informativi del firewall quando vengono rilevati tentativi di intrusione o attività sospette durante l'esecuzione di giochi a schermo intero.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avanzate** nella sezione **Avvisi**.
4. Nel riquadro Opzioni di avviso, selezionare **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**.
5. Fare clic su **OK**.

Nascondi avvisi informativi

È possibile impedire la visualizzazione degli avvisi informativi del firewall quando vengono rilevati tentativi di intrusione o attività sospette.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avanzate** nella sezione **Avvisi**.
4. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi informativi**.
5. Nel riquadro Avvisi informativi, effettuare una delle seguenti operazioni:
   - Selezionare **Non visualizzare avvisi informativi** per nascondere tutti gli avvisi informativi.
   - Cancellare un avviso da nascondere.
6. Fare clic su **OK**.

CAPITOLO 17

Configurazione della protezione del firewall

Il firewall prevede alcuni metodi per gestire la protezione e personalizzare la modalità di risposta agli eventi e agli avvisi relativi alla protezione.

Dopo avere installato il firewall per la prima volta, il livello di protezione del computer viene impostato su Automatica e per i programmi in uso è consentito l'accesso a Internet solo in uscita. Il firewall fornisce tuttavia altri livelli, a partire da quelli maggiormente restrittivi per arrivare a quelli più permissivi.

Offre inoltre l'opportunità di ricevere suggerimenti concernenti gli avvisi e l'accesso a Internet dei programmi.

In questo capitolo

Gestione dei livelli di protezione del firewall

I livelli di protezione del firewall controllano in che misura l'utente desidera gestire gli avvisi e rispondere agli stessi. Gli avvisi vengono visualizzati quando il firewall rileva traffico di rete indesiderato e connessioni a Internet in ingresso e in uscita. Per impostazione predefinita, il livello di protezione del firewall è impostato su Automatica, con accesso solo in uscita.

Se è impostato il livello di protezione Automatica e sono attivati i suggerimenti intelligenti, gli avvisi gialli offrono la possibilità di consentire o bloccare l'accesso per i programmi sconosciuti che richiedono l'accesso in ingresso. Anche se gli avvisi verdi sono disattivati per impostazione predefinita, vengono visualizzati al rilevamento di programmi noti e l'accesso è automaticamente consentito. Dopo aver ottenuto l'accesso, un programma sarà in grado di creare connessioni in uscita e di ascoltare connessioni in ingresso non richieste.

In genere, più il livello di protezione è restrittivo (Mascheramento e Standard), maggiore sarà il numero di opzioni e avvisi visualizzati che, a loro volta, dovranno essere gestiti dall'utente.

Nella tabella che segue sono riportati i tre livelli di protezione del firewall, a partire dal più restrittivo:

Livello	Descrizione
Mascheramento	Blocca tutte le connessioni a Internet in ingresso, escluse le porte aperte, nascondendo la presenza del computer su Internet. Il firewall avvisa quando un nuovo programma tenta di stabilire una connessione a Internet in uscita oppure riceve una richiesta di connessione in ingresso. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.
Standard	Esegue il monitoraggio delle connessioni in ingresso e in uscita e visualizza un avviso quando un nuovo programma tenta di accedere a Internet. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.
Automatica	Consente ai programmi l'accesso a Internet in ingresso e in uscita (completo) o solo in uscita. Il livello di protezione predefinito è Automatica e ai programmi è consentito solo l'accesso in uscita. Se a un programma viene consentito l'accesso completo, il firewall lo considera automaticamente affidabile e lo aggiunge all'elenco dei programmi consentiti nel riquadro Autorizzazioni programmi. Se a un programma è consentito solo l'accesso in uscita, il firewall lo considera automaticamente affidabile solo quando effettua una connessione a Internet in uscita. Una connessione in ingresso non viene automaticamente considerata affidabile.

Il firewall offre inoltre la possibilità di reimpostare immediatamente il livello di protezione su Automatica, consentendo l'accesso solo in uscita, dal riquadro Ripristina le impostazioni predefinite del firewall.

Come impostare il livello di protezione su Mascheramento

Il livello di protezione del firewall può essere impostato su Mascheramento per bloccare tutte le connessioni di rete in ingresso, fatta eccezione per le porte aperte, e nascondere la presenza del computer su Internet.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Mascheramento** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Nota: in modalità Mascheramento, il firewall avvisa l'utente quando nuovi programmi richiedono la connessione a Internet in uscita o ricevono richieste di connessione in ingresso.

Impostazione del livello di protezione su Standard

È possibile impostare il livello di protezione su Standard per monitorare le connessioni in ingresso e in uscita e per ricevere un avviso quando nuovi programmi tentano di effettuare l'accesso a Internet.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Standard** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Come impostare il livello di protezione su Automatica

Il livello di protezione del firewall può essere impostato su Automatica per consentire l'accesso completo o l'accesso alla rete solo in uscita.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Automatica** venga visualizzato come livello corrente.
4 Eseguire una delle seguenti operazioni:
   - Per consentire l'accesso completo alla rete in ingresso e in uscita, selezionare **Consenti accesso completo**.
   - Per consentire l'accesso alla rete solo in uscita, selezionare **Autorizza solo accesso in uscita**.
5 Fare clic su **OK**.

Nota: Autorizza solo accesso in uscita è l'opzione predefinita.

Configurazione dei suggerimenti intelligenti per gli avvisi

È possibile configurare il firewall in modo tale da includere, escludere o visualizzare suggerimenti negli avvisi quando i programmi tentano di accedere a Internet. L'attivazione dei suggerimenti intelligenti aiuta a decidere la modalità di gestione degli avvisi.

Se i suggerimenti intelligenti sono attivati e il livello di protezione è impostato su Automatica con accesso consentito solo in uscita, il firewall consente automaticamente i programmi noti e blocca i programmi potenzialmente pericolosi.

Se i suggerimenti intelligenti sono disattivati, il firewall non consente né blocca l'accesso a Internet e non fornisce indicazioni nell'avviso.

Se è impostata l'opzione di visualizzazione dei suggerimenti intelligenti, un avviso chiede di consentire o bloccare l'accesso e viene fornito un suggerimento nell'avviso.

Come attivare i suggerimenti intelligenti

È possibile attivare i suggerimenti intelligenti per fare in modo che il firewall consenta o blocchi automaticamente programmi e avvisi nel caso in cui rilevi programmi non riconosciuti e potenzialmente pericolosi.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Applica suggerimenti intelligenti**.
4. Fare clic su **OK**.

Come disattivare i suggerimenti intelligenti

È possibile disattivare i suggerimenti intelligenti per fare in modo che il firewall consenta o blocchi i programmi e avvisi nel caso in cui rilevi programmi non riconosciuti e potenzialmente pericolosi. Gli avvisi non includono tuttavia suggerimenti sulla gestione dell'accesso per i programmi. Se rileva un nuovo programma sospetto o noto come potenziale minaccia, il firewall impedisce automaticamente al programma di accedere a Internet.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Non applicare suggerimenti intelligenti**.
4. Fare clic su **OK**.

Come visualizzare i suggerimenti intelligenti

È possibile visualizzare i suggerimenti intelligenti in modo tale da mostrare solo un suggerimento negli avvisi per decidere se consentire o bloccare programmi non riconosciuti o potenzialmente pericolosi.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Mostra suggerimenti intelligenti**.
4. Fare clic su **OK**.

Ottimizzazione della protezione firewall

La protezione di un computer può risultare compromessa per diverse ragioni. Ad esempio, alcuni programmi potrebbero tentare di connettersi a Internet all'avvio di Windows®. Inoltre, utenti particolarmente esperti potrebbero rintracciare il computer, inviando un ping, per stabilire se è connesso a una rete. Potrebbero anche inviare informazioni al computer mediante il protocollo UDP sotto forma di unità di messaggi (datagrammi). Il firewall difende il computer da questo tipo di intrusioni consentendo all'utente di bloccare l'accesso a Internet da parte dei programmi all'avvio di Windows, bloccando le richieste di ping che consentono ad altri utenti di rilevare i computer connessi a una rete e di impedire ad altri utenti di inviare informazioni al computer sotto forma di unità di messaggi (datagrammi).

Le impostazioni di installazione standard includono il rilevamento automatico dei tentativi di intrusione più comuni, ad esempio attacchi o vulnerabilità che causano negazioni del servizio (DoS, Denial of Service). L'utilizzo di tali impostazioni garantisce la protezione dell'utente contro attacchi e scansioni, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni nel riquadro Rilevamento delle intrusioni.

Come proteggere il computer durante l'avvio

È possibile proteggere il computer durante l'avvio di Windows per bloccare nuovi programmi che non avevano accesso a Internet durante l'avvio e che adesso lo richiedono. Il firewall visualizza gli avvisi rilevanti per i programmi che avevano richiesto l'accesso a Internet, che è possibile consentire o bloccare.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Impostazioni protezione**, selezionare **Attiva protezione durante l'avvio di Windows**.
4. Fare clic su **OK**.

Nota: finché è abilitata la protezione all'avvio, le connessioni risultano bloccate e non viene registrata alcuna intrusione.

Come configurare le impostazioni di richieste ping

È possibile consentire o impedire ad altri utenti del computer di rilevare il computer sulla rete.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Impostazioni protezione**, effettuare una delle seguenti operazioni:
   - Selezionare **Consenti richieste ping ICMP** per consentire il rilevamento del computer sulla rete mediante richieste ping.
   - Deselezionare **Consenti richieste ping ICMP** per impedire il rilevamento del computer sulla rete mediante richieste ping.
4. Fare clic su **OK**.

Come configurare le impostazioni UDP

È possibile consentire ad altri utenti della rete di inviare unità di messaggi (datagrammi) al computer in uso mediante il protocollo UDP. Tale operazione può tuttavia essere eseguita solo se è stata chiusa una porta dei servizi di sistema per bloccare tale protocollo.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Impostazioni protezione**, effettuare una delle seguenti operazioni:
   - Selezionare **Attiva rilevamento UDP** per consentire ad altri utenti di inviare unità di messaggi (datagrammi) al proprio computer.
   - Deselezionare **Attiva rilevamento UDP** per impedire ad altri utenti di inviare unità di messaggi (datagrammi) al proprio computer.
4. Fare clic su **OK**.

Come configurare il rilevamento intrusioni

È possibile rilevare i tentativi di intrusione per proteggere il computer da attacchi e scansioni non autorizzate. Le impostazioni standard del firewall includono il rilevamento automatico dei tentativi di intrusione più comuni, quali gli attacchi di negazione di servizio (DoS, Denial of Service) o lo sfruttamento dei punti deboli, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Rilevamento delle intrusioni**.
4. In **Rileva tentativi di intrusione**, effettuare una delle seguenti operazioni:
   - Selezionare un nome per rilevare automaticamente l'attacco o la scansione.
   - Deselezionare un nome per disattivare il rilevamento automatico dell'attacco o della scansione.
5. Fare clic su **OK**.

Come configurare le impostazioni relative allo stato della protezione firewall

È possibile configurare il firewall in modo che ignori la mancata segnalazione di problemi specifici del computer a SecurityCenter.

1. Nella sezione **Informazioni su SecurityCenter** del riquadro McAfee SecurityCenter, fare clic su **Configura**.
2. Nel riquadro Configurazione di SecurityCenter, nella sezione **Stato protezione**, fare clic su **Avanzate**.
3. Nel riquadro Problemi ignorati, selezionare una o più delle seguenti opzioni:
   - **La protezione firewall è disattivata.**
   - **Il servizio firewall non è in esecuzione.**
   - **La protezione firewall non è installata nel computer.**
   - **Windows Firewall non è attivo.**
   - **Il firewall in uscita non è installato nel computer.**
4. Fare clic su **OK**.

Blocco e ripristino del firewall

Il blocco consente di bloccare immediatamente tutte le connessioni di rete, sia in ingresso che in uscita, compreso l'accesso a siti Web, posta elettronica e aggiornamenti della protezione. Il blocco equivale a scollegare i cavi di rete del computer. È possibile utilizzare questa impostazione per bloccare le porte aperte nel riquadro Servizi di sistema e isolare e risolvere un problema nel computer.

Come bloccare immediatamente il firewall

È possibile bloccare il firewall per bloccare immediatamente tutto il traffico di rete tra il computer e le reti, compresa Internet.

1 Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Blocca firewall**.
2 Nel riquadro Blocca firewall, fare clic su **Attiva blocco firewall**.
3 Fare clic su **Sì** per confermare.

Suggerimento: per bloccare il firewall è anche possibile fare clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica all'estrema destra della barra delle applicazioni, quindi fare clic su **Collegamenti rapidi** e infine su **Blocca firewall**.

Come sbloccare immediatamente il firewall

È possibile sbloccare il firewall per consentire immediatamente tutto il traffico di rete tra il computer e le reti, compresa Internet.

1 Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Blocca firewall**.
2 Nel riquadro Blocco attivato, fare clic su **Disattiva blocco firewall**.
3 Fare clic su **Sì** per confermare.

Come ripristinare le impostazioni del firewall

È possibile ripristinare rapidamente le impostazioni di protezione originali del firewall. La funzione di ripristino reimposta il livello di protezione su Automatica e consente l'accesso alla rete solo in uscita, attiva i suggerimenti intelligenti, ripristina l'elenco dei programmi predefiniti e le relative autorizzazioni nel riquadro Autorizzazioni programmi, rimuove gli indirizzi IP affidabili ed esclusi e ripristina i servizi di sistema, le impostazioni del registro eventi e il rilevamento intrusioni.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Ripristina le impostazioni predefinite del firewall**.
2. Nel riquadro Ripristina le impostazioni predefinite della protezione firewall, fare clic su **Ripristina impostazioni predefinite**.
3. Fare clic su **Sì** per confermare.
4. Fare clic su **OK**.

CAPITOLO 18

Gestione dei programmi e delle autorizzazioni

Personal Firewall consente di gestire e di creare autorizzazioni di accesso per programmi già esistenti e nuovi che richiedono accesso a Internet in ingresso e in uscita. Il firewall consente di controllare l'accesso completo o solo in uscita per i programmi, ma anche di bloccare qualsiasi tipo di accesso.

In questo capitolo

Autorizzazione di accesso a Internet per i programmi

Alcuni programmi, quali i browser Internet, devono necessariamente accedere a Internet per funzionare in modo corretto.

Personal Firewall consente di utilizzare la pagina Autorizzazioni programmi per:

- Consentire l'accesso per i programmi
- Consentire solo l'accesso in uscita per i programmi
- Bloccare l'accesso per i programmi

È inoltre possibile consentire l'accesso completo e solo in uscita a Internet per un programma dal registro Eventi in uscita ed Eventi recenti.

Come autorizzare l'accesso completo per un programma

È possibile consentire a un programma bloccato esistente nel computer di avere accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Solo accesso in uscita**.
5. In **Azione**, fare clic su **Autorizza accesso**.
6. Fare clic su **OK**.

Come autorizzare l'accesso completo per un nuovo programma

È possibile consentire a un nuovo programma del computer di avere accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, fare clic su **Aggiungi programma autorizzato**.
5. Nella finestra di dialogo **Aggiungi programma**, cercare e selezionare il programma che si desidera aggiungere, quindi fare clic su **Apri**.

Nota: è possibile modificare le autorizzazioni di un programma appena aggiunto in modo analogo a quello di un programma esistente, selezionandolo e quindi facendo clic su **Autorizza solo accesso in uscita** o su **Blocca accesso** in **Azione**.

Come autorizzare l'accesso completo dal registro Eventi recenti

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi recenti, in modo che abbia accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Autorizza accesso**.
4. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Argomenti correlati

- Come visualizzare gli eventi in uscita (pagina 113)

Come autorizzare l'accesso completo dal registro Eventi in uscita

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi in uscita in modo che abbia accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un programma, quindi in **Desidero**, fare clic su **Autorizza accesso**.
6. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Autorizzazione per l'accesso solo in uscita ai programmi

Alcuni programmi del computer richiedono l'accesso a Internet in uscita. Il firewall consente di configurare le autorizzazioni dei programmi per consentire l'accesso a Internet solo in uscita.

Come autorizzare l'accesso solo in uscita per un programma

È possibile autorizzare un programma per l'accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Accesso completo**.
5. In **Azione**, fare clic su **Autorizza solo accesso in uscita**.
6. Fare clic su **OK**.

Come autorizzare l'accesso solo in uscita dal registro Eventi recenti

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi recenti in modo che abbia accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Autorizza solo accesso in uscita**.
4. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Come autorizzare l'accesso solo in uscita dal registro Eventi in uscita

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi in uscita in modo che abbia accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un programma, quindi in **Desidero**, fare clic su **Autorizza solo accesso in uscita**.
6. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Blocco dell'accesso a Internet per i programmi

Personal Firewall consente di impedire ai programmi l'accesso a Internet. Accertarsi che il blocco di un programma non interrompa la connessione di rete o non impedisca a un altro programma che richiede l'accesso a Internet di funzionare in modo corretto.

Come bloccare l'accesso per un programma

È possibile bloccare un programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4 In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Accesso completo** o **Solo accesso in uscita**.
5 In **Azione**, fare clic su **Blocca accesso**.
6 Fare clic su **OK**.

Come bloccare l'accesso per un nuovo programma

È possibile bloccare un nuovo programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4 In **Autorizzazioni programmi**, fare clic su **Aggiungi programma bloccato**.
5 Nella finestra di dialogo Aggiungi programma, cercare e selezionare il programma che si desidera aggiungere, quindi fare clic su **Apri**.

Nota: per modificare le autorizzazioni di un programma appena aggiunto, selezionare il programma e fare clic su **Autorizza solo accesso in uscita** o su **Autorizza accesso** in **Azione**.

Come bloccare l'accesso dal registro Eventi recenti

È possibile bloccare un programma visualizzato nel registro Eventi recenti in modo che non abbia accesso a Internet in ingresso e in uscita.

1 Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2 Fare clic su **Rapporti e registri**.
3 In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Blocca accesso**.
4 Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Rimozione delle autorizzazioni di accesso per i programmi

Prima di rimuovere un'autorizzazione per un programma, accertarsi che l'eliminazione non influisca sulla funzionalità del computer o della connessione di rete.

Come rimuovere un'autorizzazione per un programma

È possibile rimuovere un programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4 Selezionare un programma in **Autorizzazioni programmi**.
5 In **Azione**, fare clic su **Rimuovi autorizzazione programma**.
6 Fare clic su **OK**.

Nota: Personal Firewall impedisce all'utente di modificare alcuni programmi visualizzando in grigio e disattivando determinate azioni.

Informazioni sui programmi

Se non si è certi dell'autorizzazione da applicare per un programma, è possibile reperire informazioni relative al programma sul sito Web HackerWatch di McAfee.

Come reperire informazioni sui programmi

È possibile reperire informazioni sui programmi sul sito Web HackerWatch di McAfee per decidere se consentire o bloccare l'accesso a Internet in ingresso e in uscita.

Nota: accertarsi di essere connessi a Internet affinché il browser possa avviare il sito Web HackerWatch di McAfee, che fornisce informazioni aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. Selezionare un programma in **Autorizzazioni programmi**.
5. In **Azione**, fare clic su **Ulteriori informazioni**.

Come reperire informazioni sui programma dal registro Eventi in uscita

Mediante il registro Eventi in uscita, è possibile ottenere le informazioni sui programmi presenti sul sito Web HackerWatch di McAfee e decidere per quali programmi consentire o bloccare l'accesso a Internet in ingresso e in uscita.

Nota: accertarsi di essere connessi a Internet affinché il browser possa avviare il sito Web HackerWatch di McAfee, che fornisce informazioni aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In Eventi recenti selezionare un evento, quindi fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un indirizzo IP, quindi fare clic su **Ulteriori informazioni**.

CAPITOLO 19

Gestione delle connessioni a computer

È possibile configurare il firewall in modo tale da gestire connessioni remote specifiche a computer mediante la creazione di regole, basate sugli indirizzi IP, associate ai computer remoti. I computer associati a indirizzi IP affidabili si possono considerare idonei alla connessione al computer in uso mentre gli indirizzi IP sconosciuti, sospetti o inattendibili, possono essere esclusi dalla connessione al computer.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili. Il firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP affidabili inclusi nell'elenco **Reti**.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché il firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione a Internet comporti una minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet.

In questo capitolo

Informazioni sulle connessioni a computer

Le connessioni a computer sono connessioni create tra altri computer di qualsiasi rete e il computer in uso. È possibile aggiungere, modificare e rimuovere gli indirizzi IP inclusi nell'elenco **Reti**. Tali indirizzi IP sono associati alle reti per le quali si desidera assegnare un livello di affidabilità durante la connessione al computer in uso: Affidabile, Standard e Pubblica.

Livello	Descrizione
Affidabile	Il firewall consente il traffico da un indirizzo IP al computer in uso attraverso qualsiasi porta. L'attività tra il computer associato a un indirizzo IP affidabile e quello in uso non viene filtrata o analizzata dal firewall. Per impostazione predefinita, nell'elenco **Reti** viene elencata come affidabile la prima rete privata rilevata dal firewall. Un esempio di rete affidabile è rappresentato da uno o più computer presenti nella rete locale o domestica.
Standard	Il firewall controlla il traffico da un solo indirizzo IP (escludendo gli altri computer in tale rete) durante la connessione al computer in uso e consente o blocca l'accesso in base alle regole configurate nell'elenco **Servizi di sistema**. Il firewall registra il traffico e genera avvisi relativi a eventi provenienti da indirizzi IP standard. Un esempio di rete standard è rappresentato da uno o più computer presenti in una rete aziendale.
Pubblica	Il firewall controlla il traffico proveniente da una rete pubblica in base alle regole configurate nell'elenco **Servizi di sistema**. Un esempio di rete pubblica è rappresentato da una rete Internet presso un Internet café, un albergo o un aeroporto.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili.

Come aggiungere una connessione a computer

È possibile aggiungere una connessione a un computer affidabile, standard o pubblico con i relativi indirizzi IP.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Reti**.
4 Nel riquadro Reti, fare clic su **Aggiungi**.
5 Se la connessione al computer è configurata su una rete IPv6, selezionare la casella di controllo **IPv6**.
6 In **Aggiungi regola**, effettuare una delle seguenti operazioni:
   - Selezionare **Singolo** e immettere l'indirizzo IP nella casella **Indirizzo IP**.
   - Selezionare **Intervallo** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**. Se la connessione al computer è configurata su una rete IPv6, immettere l'indirizzo IP iniziale e la lunghezza del prefisso nelle caselle **Da indirizzo IP** e **Lunghezza prefisso**.
7 In **Tipo**, effettuare una delle seguenti operazioni:
   - Selezionare **Affidabile** per indicare che la connessione al computer è affidabile, ad esempio nel caso di un computer in una rete domestica.
   - Selezionare **Standard** per specificare che solo la connessione al computer in uso, e non ad altri computer della stessa rete, è affidabile (ad esempio, un computer in una rete aziendale).
   - Selezionare **Pubblica** per specificare che la connessione al computer è pubblica, ad esempio se il computer è in un albergo, aeroporto o Internet café.
8 Se un servizio di sistema utilizza Condivisione connessione Internet (ICS, Internet Connection Sharing), è possibile aggiungere il seguente intervallo di indirizzi IP: da 192.168.0.1 a 192.168.0.255.
9 Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
10 Se lo si desidera, digitare una descrizione della regola.
11 Fare clic su **OK**.

Nota: per ulteriori informazioni su Condivisione connessione Internet (ICS, Internet Connection Sharing), vedere Come configurare un nuovo servizio di sistema.

Come aggiungere un computer dal registro Eventi in ingresso

È possibile aggiungere una connessione a computer affidabile o standard con il relativo indirizzo IP dal registro Eventi in ingresso.

1. Nella sezione Attività comuni del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.
5. Selezionare un indirizzo IP di origine e in **Desidero**, effettuare una delle seguenti operazioni:
   - Fare clic su **Aggiungi questo indirizzo IP come Affidabile** per aggiungere il computer come Affidabile nell'elenco **Reti**.
   - Fare clic su **Aggiungi questo indirizzo IP come Standard** per aggiungere la connessione al computer come Standard all'elenco **Reti**.
6. Fare clic su **Sì** per confermare.

Come modificare una connessione a computer

È possibile modificare una connessione a un computer affidabile, standard o pubblico con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Reti**.
4. Selezionare un indirizzo IP nel riquadro Reti, quindi fare clic su **Modifica**.
5. Se la connessione al computer è configurata su una rete IPv6, selezionare la casella di controllo **IPv6**.
6. In **Modifica regola**, effettuare una delle seguenti operazioni:
   - Selezionare **Singolo** e immettere l'indirizzo IP nella casella **Indirizzo IP**.
   - Selezionare **Intervallo** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**. Se la connessione al computer è configurata su una rete IPv6, immettere l'indirizzo IP iniziale e la lunghezza del prefisso nelle caselle **Da indirizzo IP** e **Lunghezza prefisso**.
7. In **Tipo**, effettuare una delle seguenti operazioni:
   - Selezionare **Affidabile** per indicare che la connessione al computer è affidabile, ad esempio nel caso di un computer in una rete domestica.

- Selezionare **Standard** per specificare che solo la connessione al computer in uso, e non ad altri computer della stessa rete, è affidabile (ad esempio, un computer in una rete aziendale).
- Selezionare **Pubblica** per specificare che la connessione al computer è pubblica, ad esempio se il computer è in un albergo, aeroporto o Internet café.

8. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
9. Se lo si desidera, digitare una descrizione della regola.
10. Fare clic su **OK**.

Nota: non è possibile modificare la connessione predefinita del computer che il firewall ha aggiunto automaticamente da una rete privata affidabile.

Come rimuovere una connessione a computer

È possibile rimuovere una connessione a un computer affidabile, standard o pubblico con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Reti**.
4. Selezionare un indirizzo IP nel riquadro Reti, quindi fare clic su **Rimuovi**.
5. Fare clic su **Sì** per confermare.

Esclusione delle connessioni a computer

È possibile aggiungere, modificare e rimuovere indirizzi IP esclusi nel riquadro Indirizzi IP esclusi.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché il firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione a Internet comporti una minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet.

Come aggiungere una connessione a computer escluso

È possibile aggiungere una connessione a computer escluso con i relativi indirizzi IP.

Nota: assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.

2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.

3 Nel riquadro Firewall, fare clic su **Indirizzi IP esclusi**.

4 Nel riquadro Indirizzi IP esclusi, fare clic su **Aggiungi**.

5 Se la connessione al computer è configurata su una rete IPv6, selezionare la casella di controllo **IPv6**.

6 In **Aggiungi regola**, effettuare una delle seguenti operazioni:

   - Selezionare **Singolo** e immettere l'indirizzo IP nella casella **Indirizzo IP**.
   - Selezionare **Intervallo** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**. Se la connessione al computer è configurata su una rete IPv6, immettere l'indirizzo IP iniziale e la lunghezza del prefisso nelle caselle **Da indirizzo IP** e **Lunghezza prefisso**.

7 Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.

8 Se lo si desidera, digitare una descrizione della regola.

9 Fare clic su **OK**.

10 Fare clic su **Sì** per confermare.

Come modificare una connessione a computer escluso

È possibile modificare una connessione a computer escluso con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Indirizzi IP esclusi**.
4. Nel riquadro Indirizzi IP esclusi, fare clic su **Modifica**.
5. Se la connessione al computer è configurata su una rete IPv6, selezionare la casella di controllo **IPv6**.
6. In **Modifica regola**, effettuare una delle seguenti operazioni:
   - Selezionare **Singolo** e immettere l'indirizzo IP nella casella **Indirizzo IP**.
   - Selezionare **Intervallo** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**. Se la connessione al computer è configurata su una rete IPv6, immettere l'indirizzo IP iniziale e la lunghezza del prefisso nelle caselle **Da indirizzo IP** e **Lunghezza prefisso**.
7. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
8. Se lo si desidera, digitare una descrizione della regola.
9. Fare clic su **OK**.

Come rimuovere una connessione a computer escluso

È possibile rimuovere una connessione a computer escluso con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Indirizzi IP esclusi**.
4. Selezionare un indirizzo IP nel riquadro Indirizzi IP esclusi, quindi fare clic su **Rimuovi**.
5. Fare clic su **Sì** per confermare.

Come escludere un computer dal registro Eventi in ingresso

È possibile escludere una connessione a computer con il relativo indirizzo IP dal registro Eventi in ingresso. Utilizzare il registro, che elenca gli indirizzi IP del traffico Internet in ingresso, per escludere un indirizzo IP che sembra essere l'origine di attività Internet sospette o indesiderate.

Aggiungere un indirizzo IP all'elenco **Indirizzi IP esclusi** per bloccare il traffico Internet in ingresso, indipendentemente dal fatto che le porte dei Servizi di sistema siano aperte o chiuse.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.
5. Selezionare un indirizzo IP di origine quindi, nella sezione **Desidero**, fare clic su **Escludi questo indirizzo IP**.
6. Fare clic su **Sì** per confermare.

Come escludere un computer dal registro Eventi Sistema rilevamento intrusioni

È possibile escludere una connessione a computer e il relativo indirizzo IP dal registro Eventi Sistema rilevamento intrusioni.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**.
5. Selezionare un indirizzo IP di origine quindi, nella sezione **Desidero**, fare clic su **Escludi questo indirizzo IP**.
6. Fare clic su **Sì** per confermare.

CAPITOLO 20

Gestione dei servizi di sistema

Per funzionare correttamente, alcuni programmi, tra cui i server Web o i programmi server di condivisione dei file, devono accettare connessioni non richieste da altri computer attraverso porte progettate per i servizi di sistema. In genere il firewall chiude le porte dei servizi di sistema poiché rappresentano l'origine più probabile dei problemi di protezione del sistema. Per accettare le connessioni dai computer remoti è tuttavia necessario aprire tali porte.

In questo capitolo

Configurazione delle porte dei servizi di sistema

È possibile configurare le porte dei servizi di sistema in modo da consentire o bloccare l'accesso remoto alla rete da un servizio presente sul computer. Tali porte dei servizi di sistema possono essere aperte o chiuse per computer indicati come affidabili, standard o pubblici nell'elenco **Reti**.

Nell'elenco che segue sono riportati i servizi di sistema comuni e le porte ad essi associate:

- Porta 5357 del sistema operativo comune
- Porte 20-21 di File Transfer Protocol (FTP)
- Porta 143 del server di posta (IMAP)
- Porta 110 del server di posta (POP3)
- Porta 25 del server di posta (SMTP)
- Porta 445 di Microsoft Directory Server (MSFT DS)
- Porta 1433 di Microsoft SQL Server (MSFT SQL)
- Porta 123 di Network Time Protocol
- Porta 3389 di Desktop remoto/Assistenza remota/Terminal Server (RDP)
- Porta 135 per chiamate di procedura remota (RPC)
- Porta 443 del server Web protetto (HTTPS)
- Porta 5000 di Universal Plug and Play (UPNP)
- Porta 80 del server Web (HTTP)
- Porte 137-139 per la condivisione file in Windows (NETBIOS)

È inoltre possibile configurare le porte dei servizi di sistema in modo da consentire a un computer di condividere la connessione a Internet con altri computer a cui è collegato tramite la stessa rete. Tale connessione, nota come Condivisione connessione Internet (ICS, Internet Connection Sharing), fa sì che il computer che condivide la connessione svolga la funzione di gateway per Internet per gli altri computer collegati in rete.

Nota: se nel computer è presente un'applicazione che accetta le connessioni al server Web o FTP, è possibile che il computer che condivide la connessione debba aprire la porta dei servizi di sistema associata e consentire le connessioni in ingresso e di inoltro per tali porte.

Come consentire l'accesso alla porta di un servizio di sistema esistente

È possibile aprire una porta esistente per consentire l'accesso remoto alla rete a un servizio di sistema presente sul computer in uso.

Nota: le porte dei servizi di sistema aperte possono rendere il computer vulnerabile a minacce per la protezione, pertanto devono essere aperte solo in caso di necessità.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. In **Apri porta del servizio di sistema** selezionare un servizio di sistema per aprire la porta associata.
5. Fare clic su **Modifica**.
6. Eseguire una delle seguenti operazioni:
   - Per aprire la porta su qualsiasi computer di una rete affidabile, standard o pubblica, ad esempio una rete domestica, una rete aziendale o una rete Internet, selezionare **Affidabile, Standard e Pubblica**.
   - Per aprire la porta su qualsiasi computer di una rete standard, ad esempio una rete aziendale, selezionare **Standard (comprende Affidabile)**.
7. Fare clic su **OK**.

Come bloccare l'accesso a una porta dei servizi di sistema esistente

È possibile chiudere una porta esistente per bloccare l'accesso remoto alla rete di un servizio di sistema presente sul computer in uso.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. In **Apri porta del servizio di sistema**, deselezionare la casella di controllo accanto al servizio di sistema che si desidera chiudere.
5. Fare clic su **OK**.

Come configurare una nuova porta dei servizi di sistema

È possibile configurare nel computer una nuova porta dei servizi di rete da aprire o chiudere per consentire o bloccare l'accesso remoto al computer in uso.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. Fare clic su **Aggiungi**.
5. Nel riquadro Servizi di sistema, in **Aggiungi regola servizi di sistema**, immettere quanto segue:
   - Nome servizio di sistema
   - Categoria servizio di sistema
   - Porte TCP/IP locali
   - Porte UDP locali
6. Eseguire una delle seguenti operazioni:
   - Per aprire la porta su qualsiasi computer di una rete affidabile, standard o pubblica, ad esempio una rete domestica, una rete aziendale o una rete Internet, selezionare **Affidabile, Standard e Pubblica**.
   - Per aprire la porta su qualsiasi computer di una rete standard, ad esempio una rete aziendale, selezionare **Standard (comprende Affidabile)**.
7. Se si desidera inviare le informazioni relative all'attività di tale porta a un altro computer Windows presente sulla rete, che condivide la connessione a Internet, selezionare **Inoltrare l'attività di questa porta ai computer di rete che utilizzano Condivisione connessione Internet**.
8. Se lo si desidera, descrivere la nuova configurazione.
9. Fare clic su **OK**.

Nota: se nel computer è presente un programma che accetta le connessioni al server Web o FTP, è possibile che il computer che condivide la connessione debba aprire la porta dei servizi di sistema associata e consentire le connessioni in ingresso e di inoltro per tali porte. Se si utilizza Condivisione connessione Internet (ICS, Internet Connection Sharing), è inoltre necessario aggiungere una connessione a computer affidabile all'elenco **Reti**. Per ulteriori informazioni, vedere Come aggiungere una connessione a computer.

Come modificare una porta dei servizi di sistema

È possibile modificare le informazioni di accesso alla rete in ingresso e in uscita relative a una porta dei servizi di sistema esistente.

Nota: se le informazioni sulla porta non vengono inserite in modo corretto, il servizio di sistema non funziona.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4 Selezionare la casella di controllo accanto a un servizio di sistema, quindi fare clic su **Modifica**.
5 Nel riquadro Servizi di sistema, in **Aggiungi regola servizi di sistema**, modificare quanto segue:
   - Nome servizio di sistema
   - Porte TCP/IP locali
   - Porte UDP locali
6 Eseguire una delle seguenti operazioni:
   - Per aprire la porta su qualsiasi computer di una rete affidabile, standard o pubblica, ad esempio una rete domestica, una rete aziendale o una rete Internet, selezionare **Affidabile, Standard e Pubblica**.
   - Per aprire la porta su qualsiasi computer di una rete standard, ad esempio una rete aziendale, selezionare **Standard (comprende Affidabile)**.
7 Se si desidera inviare le informazioni relative all'attività di tale porta a un altro computer Windows presente sulla rete, che condivide la connessione a Internet, selezionare **Inoltrare l'attività di questa porta ai computer di rete che utilizzano Condivisione connessione Internet**.
8 Se lo si desidera, descrivere la configurazione modificata.
9 Fare clic su **OK**.

Come rimuovere una porta dei servizi di sistema

È possibile rimuovere dal computer una porta dei servizi di sistema. Dopo la rimozione i computer remoti non saranno più in grado di accedere al servizio di rete sul computer in uso.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3 Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4 Selezionare un servizio di sistema e fare clic su **Rimuovi**.
5 Alla richiesta di conferma, fare clic su **Sì**.

CAPITOLO 21

Registrazione, monitoraggio e analisi

Il firewall fornisce registrazione, monitoraggio e analisi estesi e di facile lettura relativi a eventi e traffico Internet. La comprensione di tali argomenti agevola la gestione delle connessioni Internet.

In questo capitolo

Registrazione eventi

Il firewall consente di attivare o disattivare la registrazione e, nel primo caso, specificare i tipi di eventi da registrare. Grazie alla registrazione degli eventi è possibile visualizzare gli eventi recenti in ingresso, in uscita e gli eventi di intrusione.

Come configurare le impostazioni del registro eventi

È possibile specificare e configurare i tipi di eventi del firewall da registrare. Per impostazione predefinita la registrazione degli eventi è attivata per tutti gli eventi e le attività.

1. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Impostazioni registro eventi**.
3. Se non è già selezionato, selezionare **Attiva registrazione eventi**.
4. In **Attiva registrazione eventi**, selezionare o deselezionare i tipi di eventi che si desidera o non si desidera registrare. Tra i tipi di eventi sono inclusi:
   - Programmi bloccati
   - Ping ICMP
   - Traffico da indirizzi IP esclusi
   - Eventi su porte dei servizi di sistema
   - Eventi su porte sconosciute
   - Eventi del Sistema di rilevamento intrusioni (IDS, Intrusion Detection System)
5. Per impedire la registrazione su determinate porte, selezionare **Non registrare gli eventi sulle porte seguenti**, quindi immettere i singoli numeri di porta separati da virgole o intervalli separati da trattini, ad esempio: `137-139, 445, 400-5000`.
6. Fare clic su **OK**.

Come visualizzare gli eventi recenti

Quando l'accesso è attivato, è possibile visualizzare gli eventi recenti. Nel riquadro Eventi recenti sono visualizzate la data e la descrizione dell'evento. Viene visualizzata l'attività dei programmi per i quali è stato esplicitamente bloccato l'accesso a Internet.

- Nel riquadro Attività comuni del **Menu avanzato**, fare clic su **Rapporti e registri** o su **Visualizza eventi recenti**. In alternativa, fare clic su **Visualizza eventi recenti** nel riquadro Attività comuni dal menu standard.

Come visualizzare gli eventi in ingresso

Quando l'accesso è attivato, è possibile visualizzare gli eventi in ingresso. Gli eventi in ingresso comprendono la data e l'ora, l'indirizzo IP, il nome host nonché il tipo di evento e di informazioni.

1 Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2 In **Eventi recenti**, fare clic su **Visualizza registro**.
3 Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.

Nota: un indirizzo IP può essere impostato come affidabile, escluso e rintracciato dal registro Eventi in ingresso.

Come visualizzare gli eventi in uscita

Quando l'accesso è attivato, è possibile visualizzare gli eventi in uscita. Gli eventi in uscita includono il nome del programma che tenta l'accesso in uscita, la data e l'ora dell'evento e il percorso del programma sul computer.

1 Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2 In **Eventi recenti**, fare clic su **Visualizza registro**.
3 Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.

Nota: è possibile consentire l'accesso completo e solo in uscita a un programma dal registro Eventi in uscita, nonché individuare ulteriori informazioni relative al programma.

Come visualizzare gli eventi di rilevamento intrusioni

Quando l'accesso è attivato, è possibile visualizzare gli eventi di intrusione in ingresso. Gli eventi di rilevamento intrusioni visualizzano la data e l'ora, l'IP di origine, il nome host dell'evento e il tipo di evento.

1 Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2 In **Eventi recenti**, fare clic su **Visualizza registro**.
3 Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**.

Nota: un indirizzo IP può essere escluso e rintracciato dal registro Eventi Sistema rilevamento intrusioni.

Utilizzo delle statistiche

Il firewall sfrutta il sito Web della protezione HackerWatch di McAfee per fornire statistiche sugli eventi di protezione e l'attività delle porte Internet globali.

Come visualizzare le statistiche globali sugli eventi di protezione

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni registrate elencano gli incidenti segnalati a HackerWatch nel corso delle ultime 24 ore, degli ultimi 7 giorni e degli ultimi 30 giorni.

1 Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2 Nel riquadro Strumenti, fare clic su **HackerWatch**.
3 In Traccia degli eventi, visualizzare le statistiche sugli eventi di protezione.

Come visualizzare l'attività globale delle porte Internet

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni visualizzate includono gli eventi principali relativi alle porte segnalati in HackerWatch durante gli ultimi sette giorni. In genere vengono visualizzate le informazioni sulle porte HTTP, TCP e UDP.

1 Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2 Nel riquadro Strumenti, fare clic su **HackerWatch**.
3 Visualizzare gli eventi principali relativi alle porte in **Attività recente sulle porte**.

Rintracciamento del traffico Internet

Il firewall prevede alcune opzioni per rintracciare il traffico Internet, che consentono di rintracciare geograficamente un computer di rete, ottenere informazioni relative a dominio e rete e rintracciare i computer dai registri Eventi in ingresso ed Eventi Sistema di rilevamento intrusioni.

Come rintracciare geograficamente un computer di rete

È possibile utilizzare il tracciato visivo per individuare geograficamente un computer che è connesso o tenta di connettersi al computer in uso, tramite il nome o l'indirizzo IP, nonché per accedere alle informazioni sulla rete e ai dati per la registrazione. L'esecuzione del tracciato visivo consente di visualizzare il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer e fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione mappa**.

Nota: non è possibile registrare eventi da indirizzi IP di loopback, privati o non validi.

Come ottenere i dati per la registrazione del computer

È possibile ottenere i dati per la registrazione di un computer da SecurityCenter tramite Tracciato visivo. Le informazioni includono il nome del dominio, il nome e l'indirizzo dell'intestatario e il contatto amministrativo.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione intestatario dominio**.

Come ottenere informazioni sulla rete del computer

È possibile ottenere informazioni sulla rete di un computer da SecurityCenter tramite Tracciato visivo. Tali informazioni includono dettagli sulla rete in cui risiede il dominio in questione.

1 Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2 Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3 Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4 In **Tracciato visivo**, selezionare **Visualizzazione rete**.

Come rintracciare un computer dal registro Eventi in ingresso

Dal riquadro Eventi in ingresso, è possibile rintracciare un indirizzo IP visualizzato nel registro Eventi in ingresso.

1 Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2 In **Eventi recenti**, fare clic su **Visualizza registro**.
3 Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.
4 Nel riquadro Eventi in ingresso, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo IP**.
5 Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
6 Fare clic su **Fine**.

Come rintracciare un computer dal registro Eventi Sistema rilevamento intrusioni

Dal riquadro Eventi Sistema rilevamento intrusioni, è possibile rintracciare un indirizzo IP visualizzato nell'omonimo registro.

1. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**. Nel riquadro Eventi Sistema rilevamento intrusioni, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo IP**.
4. Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
5. Fare clic su **Fine**.

Come rintracciare un indirizzo IP monitorato

È possibile rintracciare un indirizzo IP monitorato per ottenere una visualizzazione geografica indicante il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. Selezionare un programma e l'indirizzo IP visualizzato sotto il nome del programma.
5. In **Attività programmi**, fare clic su **Rintraccia questo indirizzo IP**.
6. Nella sezione **Tracciato visivo** è possibile visualizzare una mappa che indica il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Tracciato visivo**.

Monitoraggio del traffico Internet

Personal Firewall prevede alcuni metodi di monitoraggio del traffico Internet, tra cui:

- **Grafico analisi traffico**: visualizza il traffico Internet recente in entrata e in uscita.
- **Grafico utilizzo traffico**: visualizza la percentuale di larghezza di banda utilizzata dalle applicazioni maggiormente attive durante le ultime 24 ore.
- **Programmi attivi**: visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Informazioni sul grafico analisi traffico

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Il Controllo traffico visualizza inoltre i programmi utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Dal riquadro Analisi traffico è possibile visualizzare il traffico Internet, in ingresso e in uscita, con velocità di trasferimento corrente, media e massima. È inoltre possibile visualizzare il volume del traffico, compresi la quantità di traffico dall'avvio del firewall e il traffico complessivo relativo al mese in corso e ai precedenti.

Il riquadro Analisi traffico mostra l'attività Internet in tempo reale nel computer in uso, inclusi il volume e la velocità di traffico Internet recente, in ingresso e in uscita, la velocità di connessione e i byte totali trasferiti attraverso Internet.

La linea verde continua rappresenta la velocità di trasferimento corrente del traffico in ingresso. La linea verde tratteggiata rappresenta la velocità di trasferimento media del traffico in ingresso. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

La linea rossa continua rappresenta la velocità di trasferimento corrente del traffico in uscita. La linea rossa tratteggiata rappresenta la velocità di trasferimento media del traffico in uscita. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

Come analizzare il traffico in ingresso e in uscita

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Il Controllo traffico visualizza inoltre i programmi utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Analisi traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Analisi traffico**.

Come monitorare la larghezza di banda dei programmi

È possibile visualizzare il grafico a torta che mostra la percentuale approssimativa di larghezza di banda utilizzata dai programmi più attivi presenti nel computer durante le ultime ventiquattro ore. Il grafico a torta fornisce la rappresentazione visiva delle quantità di larghezza di banda relative utilizzate dai programmi.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Utilizzo traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Utilizzo traffico**.

Come monitorare l'attività dei programmi

È possibile visualizzare l'attività dei programmi in ingresso e in uscita in cui vengono mostrate le connessioni e le porte del computer remoto.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. È possibile visualizzare le seguenti informazioni:
   - Grafico attività programmi: selezionare un programma per visualizzare il grafico della relativa attività.
   - Connessione in ascolto: selezionare un elemento in ascolto sotto il nome del programma.
   - Connessione al computer: selezionare un indirizzo IP sotto il nome del programma, il processo di sistema o il servizio.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Programmi attivi**.

CAPITOLO 22

Informazioni sulla protezione Internet

Il firewall utilizza il sito Web della protezione di McAfee, HackerWatch, per fornire informazioni aggiornate sui programmi e sull'attività Internet globale. HackerWatch prevede inoltre un'esercitazione HTML relativa al firewall.

In questo capitolo

Come avviare l'esercitazione HackerWatch

Per ottenere ulteriori informazioni sul firewall, è possibile accedere all'esercitazione HackerWatch da SecurityCenter.

1 Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2 Nel riquadro Strumenti, fare clic su **HackerWatch**.
3 In **Risorse di HackerWatch**, fare clic su **Visualizza esercitazione**.

CAPITOLO 23

McAfee Anti-Spam

Anti-Spam (già SpamKiller) impedisce che la posta elettronica indesiderata entri nella cartella della posta in arrivo esaminando i messaggi in arrivo e classificandoli come posta indesiderata (messaggi che propongono un acquisto) o come phishing (messaggi che chiedono di fornire informazioni personali a un sito Web potenzialmente fraudolento). Anti-Spam filtra la posta indesiderata e la sposta nella cartella McAfee Anti-Spam.

Se un amico invia un messaggio di posta elettronica legittimo che può sembrare posta indesiderata, è possibile fare in modo che tale messaggio non venga filtrato aggiungendo l'indirizzo del mittente all'elenco degli amici di Anti-Spam. È anche possibile personalizzare la modalità di rilevamento della posta indesiderata. Ad esempio, è possibile filtrare i messaggi con maggiore severità, specificare che cosa cercare nel messaggio e creare filtri personalizzati.

Anti-Spam protegge inoltre il computer quando si tenta di accedere a un sito Web potenzialmente fraudolento da un collegamento contenuto in un messaggio di posta elettronica. Quando si fa clic su un collegamento a un sito Web potenzialmente fraudolento, si viene reindirizzati alla pagina del filtro antiphishing. Se vi sono siti Web che non si desidera filtrare, è possibile aggiungerli all'elenco indirizzi attendibili, che non vengono filtrati.

Anti-Spam può essere utilizzato con vari programmi di posta elettronica quali Yahoo®, MSN®/Hotmail®, Windows® Mail e Live™ Mail, Microsoft® Outlook®, Outlook Express e Mozilla Thunderbird™, oltre a numerosi account di posta elettronica quali POP3, POP3 Webmail e MAPI (Microsoft Exchange Server). Se si utilizza un browser per leggere la posta elettronica, è necessario aggiungere l'account Web mail ad Anti-Spam. Tutti gli altri account vengono configurati automaticamente e non è necessario aggiungerli ad Anti-Spam.

Al termine dell'installazione, non è necessario configurare Anti-Spam. Gli utenti più esperti possono tuttavia ottimizzare le funzionalità avanzate di protezione da posta indesiderata e phishing in base alle preferenze personali.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Anti-Spam

Filtri antispam	Impediscono ai messaggi di posta non richiesti di raggiungere la cartella Posta in arrivo. I filtri avanzati di Anti-Spam vengono aggiornati automaticamente per tutti gli account di posta elettronica. È inoltre possibile creare dei filtri personalizzati per assicurare che tutta la posta indesiderata venga filtrata, nonché segnalare la posta indesiderata a McAfee perché la esamini.
Filtro antiphishing	Identifica potenziali siti Web di phishing che richiedono in modo fraudolento l'invio di informazioni personali.
Elaborazione personalizzata della posta indesiderata	La posta non richiesta viene contrassegnata come posta indesiderata e inserita nella cartella McAfee Anti-Spam mentre la posta elettronica legittima viene contrassegnata come tale e inserita nella cartella della posta in arrivo.
Amici	Gli indirizzi di posta elettronica degli amici vengono importati nell'elenco degli amici in modo che i loro messaggi non vengano filtrati.

CAPITOLO 24

Configurazione del rilevamento della posta indesiderata

Anti-Spam consente di personalizzare la modalità di rilevamento della posta indesiderata. È possibile filtrare i messaggi con maggiore severità, specificare gli elementi da cercare nel messaggio nonché cercare set di caratteri specifici durante l'analisi della posta indesiderata. Anti-Spam consente inoltre di creare filtri personali per definire quali messaggi devono essere identificati come posta indesiderata. Ad esempio, se i messaggi di posta elettronica indesiderata che contengono la parola mutuo non vengono filtrati, è possibile aggiungere un filtro che contiene la parola mutuo.

Qualora vi siano dei problemi con la posta elettronica, è possibile disattivare la protezione da posta indesiderata per risolvere il problema.

In questo capitolo

Impostazione delle opzioni di filtraggio

Regolare le opzioni di filtraggio di Anti-Spam se si desidera filtrare i messaggi con maggiore severità, specificare le modalità di elaborazione dei messaggi indesiderati nonché cercare set di caratteri specifici durante l'analisi della posta indesiderata.

Livello di filtraggio

Il livello di filtraggio determina la severità con cui viene filtrata la posta elettronica. Ad esempio, se si nota che la posta indesiderata non viene filtrata e il livello di filtraggio è impostato su Medio, è possibile impostarlo su Medio-alto o Alto. Quando il livello di filtraggio è impostato su Alto, vengono accettati solo i messaggi dei mittenti inclusi nell'elenco degli amici mentre tutti gli altri vengono filtrati.

Elaborazione della posta indesiderata

Anti-Spam consente di personalizzare numerose opzioni di elaborazione della posta indesiderata. Ad esempio, è possibile inserire i messaggi indesiderati e di phishing in cartelle specifiche, modificare il nome del tag visualizzato nella riga dell'oggetto dei messaggi di posta indesiderata e di phishing, specificare una dimensione massima da filtrare e la frequenza di aggiornamento delle regole per la posta indesiderata.

Set di caratteri

Anti-Spam è in grado di cercare set di caratteri specifici durante l'analisi della posta indesiderata. I set di caratteri vengono utilizzati per rappresentare una lingua, compresi l'alfabeto, le cifre numeriche e altri simboli. Se si riceve posta indesiderata in greco, è possibile filtrare tutti i messaggi che contengono il set di caratteri greco.

Fare attenzione a non filtrare i set di caratteri delle lingue in cui si ricevono messaggi di posta elettronica autorizzati. Ad esempio, se si desidera filtrare solo i messaggi in tedesco, si potrebbe scegliere di selezionare Europa occidentale, perché la Germania fa parte dell'Europa occidentale. Se tuttavia si ricevono messaggi di posta elettronica autorizzati in italiano, quando si seleziona Europa occidentale verranno filtrati anche i messaggi in italiano e in tutte le altre lingue del set di caratteri Europa occidentale. In questo caso non è possibile filtrare solo i messaggi in tedesco.

Nota: l'impostazione del filtro dei set di caratteri è consigliata agli utenti più esperti.

Come modificare il livello di filtraggio

È possibile modificare il livello di severità con cui si desidera filtrare i messaggi di posta elettronica. Ad esempio, in caso di filtraggio di messaggi di posta elettronica autorizzati, il livello può essere abbassato.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Opzioni di filtraggio**.

3 Nell'elenco **Specificare un livello di filtro della posta indesiderata**, selezionare il livello appropriato, quindi fare clic su **OK**.

Livello	Descrizione
Basso	Viene accettata la maggior parte dei messaggi di posta elettronica.
Medio-basso	Vengono filtrati solo i messaggi chiaramente indesiderati.
Medio (consigliato)	La posta elettronica viene filtrata al livello consigliato.
Medio-alto	Tutti i messaggi di posta elettronica che sembrano essere posta indesiderata vengono filtrati.
Alto	Vengono accettati solo i messaggi provenienti da mittenti presenti nell'elenco degli amici.

Come modificare la modalità di elaborazione e classificazione della posta indesiderata

È possibile specificare una cartella in cui inserire i messaggi indesiderati e di phishing, modificare il nome del tag [SPAM] o [PHISH] visualizzato nella riga dell'oggetto dei messaggi di posta elettronica, specificare una dimensione massima da filtrare e definire la frequenza di aggiornamento delle regole per la posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Opzioni di filtraggio**.

3 Modificare o selezionare le opzioni appropriate riportate di seguito, quindi fare clic su **OK**.

Per...	Procedere come segue...
Specificare il percorso in cui collocare i messaggi indesiderati e di phishing	Selezionare una cartella dell'elenco **Colloca messaggi di posta indesiderati nella cartella**. La cartella predefinita è McAfee Anti-Spam.
Modificare la riga dell'oggetto dei messaggi di posta indesiderata	In **Contrassegna l'oggetto dei messaggi di posta indesiderata con**, specificare un tag da aggiungere alla riga dell'oggetto dei messaggi di posta indesiderata. Il tag predefinito è [SPAM].
Modificare la riga dell'oggetto dei messaggi di phishing	In **Contrassegna l'oggetto dei messaggi di posta di tipo phishing con**, specificare un tag da aggiungere alla riga dell'oggetto dei messaggi di phishing. Il tag predefinito è [PHISH].
Specificare la dimensione massima dei messaggi di posta elettronica da filtrare	In **Specificare la dimensione massima (in KB) dei messaggi di posta elettronica da filtrare**, immettere la dimensione massima dei messaggi di posta elettronica che si desidera filtrare.

Per...	Procedere come segue...
Aggiornare le regole per la posta indesiderata	Selezionare **Aggiorna regole posta indesiderata (in minuti)**, quindi immettere la frequenza di aggiornamento delle regole per la posta indesiderata. Il valore consigliato è 30 minuti. Se si dispone di una connessione di rete veloce, per ottenere risultati ottimali è possibile specificare una frequenza maggiore, ad esempio 5 minuti.
Non aggiornare le regole per la posta indesiderata	Selezionare **Non aggiornare regole posta indesiderata**.

Come applicare i filtri per i set di caratteri

Nota: il filtraggio dei messaggi che contengono caratteri di uno specifico set di caratteri è consigliato agli utenti più esperti.

È possibile filtrare un set di caratteri specifico, tuttavia fare attenzione a non filtrare il set di caratteri delle lingue in cui si riceve la posta elettronica autorizzata.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Set di caratteri**.

3 Selezionare le caselle di controllo adiacenti ai set di caratteri da filtrare.

4 Fare clic su **OK**.

Utilizzo dei filtri personali

Un filtro personale determina se bloccare o consentire i messaggi di posta elettronica in base a parole o frasi specifiche. Se un messaggio di posta elettronica contiene una parola o una frase impostata nel filtro per essere bloccata, il messaggio viene contrassegnato come posta indesiderata e lasciato nella cartella Posta in arrivo oppure inserito nella cartella McAfee Anti-Spam. Per ulteriori informazioni sulla modalità di gestione della posta indesiderata, vedere Come modificare la modalità di elaborazione e classificazione della posta indesiderata (pagina 130).

Anti-Spam include un filtro avanzato per impedire la ricezione dei messaggi indesiderati nella casella Posta in arrivo. Se si desidera tuttavia definire quali messaggi devono essere identificati come posta indesiderata, è possibile creare un filtro personale. Se ad esempio si aggiunge un filtro che contiene la parola mutuo, il filtro Anti-Spam filtrerà i messaggi che contengono tale parola. Non creare filtri che contengono parole comuni che compaiono nei messaggi di posta elettronica legittimi, altrimenti verrà filtrata anche la posta elettronica autorizzata. Dopo la creazione del filtro è possibile modificarlo se si nota che non rileva alcuni messaggi di posta indesiderata. Ad esempio, se è stato creato un filtro che cerca la parola viagra nell'oggetto del messaggio, ma si ricevono ancora messaggi che contengono tale parola perché questa è inserita nel corpo del messaggio, modificare il filtro in modo che cerchi la parola viagra nel corpo del messaggio anziché nell'oggetto.

Le espressioni regolari (RegEx) sono caratteri e sequenze speciali che possono essere utilizzate anche nei filtri personali. L'utilizzo delle espressioni regolari è tuttavia consigliato solo agli utenti più esperti. Se non si ha familiarità con le espressioni regolari o si desiderano ulteriori informazioni sul relativo utilizzo, è possibile eseguire una ricerca sul Web (ad esempio, andare a http://en.wikipedia.org/wiki/Regular_expression).

Come aggiungere un filtro personale

È possibile aggiungere dei filtri personali per definire quali messaggi devono essere identificati come posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Filtri personali**.

3 Fare clic su **Aggiungi**.

4 Specificare gli elementi che il filtro personale deve cercare (pagina 134) nel messaggio di posta elettronica.

5 Fare clic su **OK**.

Come modificare un filtro personale

Modificare i filtri esistenti per definire quali messaggi identificare come posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Filtri personali**.

3 Selezionare il filtro da modificare, quindi fare clic su **Modifica**.

4 Specificare gli elementi che il filtro personale deve cercare (pagina 134) nel messaggio di posta elettronica.

5 Fare clic su **OK**.

Come rimuovere un filtro personale

È possibile rimuovere definitivamente i filtri che non si desidera più utilizzare.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Filtri personali**.

3 Selezionare il filtro da rimuovere, quindi fare clic su **Rimuovi**.

4 Fare clic su **OK**.

Come specificare un filtro personale

La tabella descrive gli elementi ricercati dal filtro personale nel messaggio di posta elettronica.

Per...	Procedere come segue...
Specificare la parte del messaggio di posta elettronica da filtrare	Nell'elenco **Parte del messaggio di posta elettronica**, fare clic su una voce per determinare se il filtro cerca le parole o le frasi nell'oggetto, nel corpo, nell'intestazione oppure nel mittente. Nell'elenco **Parte del messaggio di posta elettronica**, fare clic su una voce per determinare se il filtro cerca un messaggio che contiene, oppure non contiene, le parole o frasi specificate.
Specificare le parole o frasi nel filtro	In **Parole o frasi**, immettere gli elementi da ricercare in un messaggio di posta elettronica. Ad esempio, se si specifica *mutuo*, verranno filtrati tutti i messaggi contenenti tale parola.
Specificare che il filtro utilizza le espressioni regolari	Selezionare **Il filtro utilizza le espressioni regolari**.
Selezionare se bloccare o consentire i messaggi di posta in base alle parole o frasi del filtro	In **Esegui l'azione**, selezionare **Blocca** o **Consenti** per bloccare o consentire i messaggi di posta contenenti le parole o frasi nel filtro.

Come disattivare la protezione da posta indesiderata

È possibile disattivare la protezione da posta indesiderata per impedire che Anti-Spam filtri la posta elettronica.

1 Nel menu avanzato, fare clic su **Configura**.
2 Nel riquadro Configura, fare clic su **Posta elettronica e MI**.
3 In **Protezione da posta indesiderata attivata**, fare clic su **Disattiva**.

Suggerimento: ricordare di fare clic su **Attiva** in **Protezione da posta indesiderata disattivata** in modo da essere protetti dalla posta indesiderata.

CAPITOLO 25

Filtraggio della posta elettronica

Anti-Spam esamina la posta in arrivo e la classifica come posta indesiderata (messaggi che propongono un acquisto) o come phishing (messaggi che chiedono di fornire informazioni personali a un sito Web potenzialmente fraudolento). Per impostazione predefinita, Anti-Spam contrassegna quindi i messaggi indesiderati come posta indesiderata o phishing (nella riga dell'oggetto del messaggio viene visualizzato il tag [SPAM] o [PHISH]) e li sposta nella cartella McAfee Anti-Spam.

È possibile contrassegnare la posta elettronica come posta indesiderata o posta autorizzata dalla barra degli strumenti di Anti-Spam, modificare la posizione in cui vengono spostati i messaggi indesiderati o modificare il tag visualizzato nella riga dell'oggetto.

È inoltre possibile disattivare le barre degli strumenti di Anti-Spam per risolvere eventuali problemi del programma di posta elettronica.

In questo capitolo

Come contrassegnare un messaggio dalla barra degli strumenti di Anti-Spam

Se un messaggio viene contrassegnato come posta indesiderata, all'oggetto del messaggio viene assegnato un tag [SPAM] o un altro tag a scelta e il messaggio rimane nella cartella Posta in arrivo, nella cartella McAfee Anti-Spam (Outlook, Outlook Express, Windows Mail, Thunderbird) o nella cartella Posta indesiderata (Eudora®). Quando un messaggio è contrassegnato come posta non indesiderata, il relativo tag viene rimosso e il messaggio viene spostato in Posta in arrivo.

Per contrassegnare un messaggio in	Selezionare un messaggio, quindi
Outlook, Outlook Express, Windows Mail	Fare clic su **Contrassegna come posta indesiderata** o **Contrassegna come posta non indesiderata**.

Per contrassegnare un messaggio in	Selezionare un messaggio, quindi
Eudora	Nel menu **Anti-Spam**, fare clic su **Contrassegna come posta indesiderata** o **Contrassegna come posta non indesiderata**.
Thunderbird	Nella barra degli strumenti di **Anti-Spam**, fare clic su **M**, quindi su **Contrassegna come** e infine scegliere **Posta indesiderata** o **Posta non indesiderata**.

Come disattivare la barra degli strumenti di Anti-Spam

Se si utilizza Outlook, Outlook Express, Windows Mail, Eudora o Thunderbird, è possibile disattivare la barra degli strumenti di Anti-Spam.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Barre degli strumenti posta elettronica**.

3 Deselezionare la casella di controllo accanto alla barra degli strumenti che si desidera disattivare.

4 Fare clic su **OK**.

Suggerimento: è possibile riattivare le barre degli strumenti di Anti-Spam in qualsiasi momento selezionando le caselle di controllo corrispondenti.

CAPITOLO 26

Impostazione degli amici

Grazie al filtro migliorato di Anti-Spam che riconosce e autorizza i messaggi di posta elettronica legittimi, raramente è necessario aggiungere gli indirizzi di posta elettronica degli amici all'elenco degli amici, sia che vengano aggiunti manualmente sia che si importino le rubriche. Se tuttavia si aggiunge l'indirizzo di posta elettronica di un amico e tale indirizzo viene contraffatto da un utente malintenzionato, Anti-Spam autorizzerà i messaggi provenienti da tale indirizzo di posta nella casella Posta in arrivo.

Se si desidera importare le rubriche e si apportano modifiche, è necessario importarle nuovamente poiché Anti-Spam non aggiorna automaticamente l'elenco degli amici.

È inoltre possibile aggiornare manualmente l'elenco degli amici di Anti-Spam, oppure aggiungere un intero dominio se si desidera che tutti gli utenti del dominio siano aggiunti all'elenco degli amici. Ad esempio, se si aggiunge il dominio azienda.com, nessun messaggio di posta elettronica proveniente da tale organizzazione verrà filtrato.

In questo capitolo

Come importare una rubrica

Importare le rubriche se si desidera che Anti-Spam aggiunga tutti gli indirizzi di posta elettronica all'elenco degli amici.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Nel riquadro Amici, fare clic su **Importa**.

4 Fare clic sul tipo di rubrica che si desidera importare nell'elenco **Selezionare una rubrica da importare**.

5 Fare clic su **Importa adesso**.

Impostazione manuale degli amici

Per aggiornare manualmente l'elenco degli amici è necessario modificare le singole voci. Ad esempio, se si riceve un messaggio di posta elettronica da un amico il cui indirizzo non è nella rubrica, è possibile aggiungere subito l'indirizzo manualmente. Il modo più semplice per farlo è utilizzare la barra degli strumenti di Anti-Spam, in caso contrario sarà necessario specificare le informazioni relative all'amico.

Come aggiungere un amico dalla barra degli strumenti di Anti-Spam

Se si utilizzano i programmi di posta elettronica Outlook, Outlook Express, Windows Mail, Eudora™ o Thunderbird, è possibile aggiungere amici direttamente dalla barra degli strumenti di Anti-Spam.

Per aggiungere un amico in	Selezionare un messaggio, quindi
Outlook, Outlook Express, Windows Mail	Fare clic su **Aggiungi amico**.
Eudora	Nel menu **Anti-Spam** fare clic su **Aggiungi amico**.

Per aggiungere un amico in	Selezionare un messaggio, quindi
Thunderbird	Nella barra degli strumenti di **Anti-Spam**, fare clic su **M**, quindi su **Contrassegna come** e infine scegliere **Amico**.

Come aggiungere un amico manualmente

Se non si desidera aggiungere un amico direttamente dalla barra degli strumenti oppure si è dimenticato di farlo quando si è ricevuto il messaggio, è possibile aggiungere una voce all'elenco degli amici.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Nel riquadro Amici, fare clic su **Aggiungi**.

4 Immettere il nome dell'amico nella casella **Nome**.

5 Selezionare **Indirizzo di posta elettronica singolo** dall'elenco **Tipo**.

6 Digitare l'indirizzo di posta elettronica dell'amico nella casella **Indirizzo di posta elettronica**.

7 Fare clic su **OK**.

Come aggiungere un dominio

Se si desidera aggiungere tutti gli utenti di un dominio all'elenco degli amici, aggiungere l'intero dominio. Ad esempio, se si aggiunge il dominio azienda.com, nessun messaggio di posta elettronica proveniente dal tale organizzazione verrà filtrato.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Nel riquadro Amici, fare clic su **Aggiungi**.

4 Digitare il nome dell'organizzazione o del gruppo nella casella **Nome**.

5 Selezionare **Intero dominio** dall'elenco **Tipo**.

6 Digitare il nome del dominio nella casella **Indirizzo di posta elettronica**.

7 Fare clic su **OK**.

Come modificare un amico

Se le informazioni relative a un amico vengono modificate, è possibile aggiornare l'elenco degli amici in modo che Anti-Spam non contrassegni i messaggi corrispondenti come posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Selezionare l'amico da modificare, quindi fare clic su **Modifica**.

4 Modificare il nome dell'amico nella casella **Nome**.

5 Modificare l'indirizzo di posta elettronica dell'amico nella casella **Indirizzo di posta elettronica**.

6 Fare clic su **OK**.

Come modificare un dominio

Se le informazioni relative a un dominio vengono modificate, è possibile aggiornare l'elenco degli amici in modo che Anti-Spam non contrassegni i messaggi provenienti da tale dominio come posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Nel riquadro Amici, fare clic su **Aggiungi**.

4 Modificare il nome dell'organizzazione o del gruppo nella casella **Nome**.

5 Selezionare **Intero dominio** dall'elenco **Tipo**.

6 Modificare il nome del dominio nella casella **Indirizzo di posta elettronica**.

7 Fare clic su **OK**.

Come rimuovere un amico

Se si riceve posta indesiderata da una persona o un dominio inclusi nell'elenco degli amici, rimuoverli dall'elenco degli amici in modo che i messaggi corrispondenti vengano filtrati.

1 Aprire il riquadro Protezione da posta indesiderata.

   In che modo?

   1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
   2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
   3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Amici**.

3 Selezionare l'amico da rimuovere, quindi fare clic su **Rimuovi**.

CAPITOLO 27

Impostazione di account Web mail

Se si utilizza un browser per leggere i messaggi di posta elettronica, è necessario configurare Anti-Spam perché si connetta all'account e filtri i messaggi. Per aggiungere l'account Web mail ad Anti-Spam, è sufficiente aggiungere le informazioni sull'account fornite dal provider del servizio di posta elettronica.

Dopo aver aggiunto l'account Web mail, è possibile modificare le informazioni dell'account e ottenere ulteriori informazioni sulla posta elettronica Web mail filtrata. Se non si utilizza più l'account Web mail oppure se non desidera filtrarlo, è possibile rimuoverlo.

Anti-Spam può essere utilizzato con vari programmi di posta elettronica quali Yahoo!®, MSN®/Hotmail®, Windows® Mail e Live™ Mail, Microsoft® Outlook®, Outlook Express e Mozilla Thunderbird™, oltre a numerosi account di posta elettronica quali POP3, POP3 Webmail e MAPI (Microsoft Exchange Server). POP 3 è il tipo di account più comune e rappresenta lo standard della posta elettronica Internet. Se si dispone di un account POP3, Anti-Spam si collega direttamente al server di posta elettronica e filtra i messaggi prima che vengano recuperati dall'account Web mail. Gli account POP3 Webmail, Yahoo!, MSN/Hotmail e Windows Mail sono basati sul Web. Il filtraggio degli account POP3 Webmail è simile a quello degli account POP3.

In questo capitolo

Come aggiungere un account Web mail

Aggiungere un account Web mail POP3 (ad esempio, Yahoo), MSN/Hotmail o Windows Mail (solo le versioni acquistate sono supportate completamente) se si desidera filtrare i messaggi di tale account per isolare la posta indesiderata.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Account Web mail**.

3 Nel riquadro Account Web mail, fare clic su **Aggiungi**.

4 Specificare le informazioni account (pagina 148), quindi fare clic su **Avanti**.

5 In **Opzioni di controllo**, specificare i tempi di controllo della posta indesiderata per l'account da parte di Anti-Spam (pagina 148).

6 Se si utilizza una connessione remota, specificare la modalità di connessione di Anti-Spam a Internet (pagina 148).

7 Fare clic su **Fine**.

Come modificare un account Web mail

Se vi sono modifiche all'account Web mail è necessario modificare le informazioni sull'account. Ad esempio, modificare l'account Web mail se si cambia la password o se si desidera che Anti-Spam controlli la posta indesiderata più spesso.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Account Web mail**.

3 Selezionare l'account da modificare, quindi fare clic su **Modifica**.

4 Specificare le informazioni account (pagina 148), quindi fare clic su **Avanti**.

5 In **Opzioni di controllo**, specificare i tempi di controllo della posta indesiderata per l'account da parte di Anti-Spam (pagina 148).

6 Se si utilizza una connessione remota, specificare la modalità di connessione di Anti-Spam a Internet (pagina 148).

7 Fare clic su **Fine**.

Come rimuovere un account Web mail

Rimuovere un account Web mail se non si desidera più filtrare la posta elettronica per la posta indesiderata. Ad esempio, se l'account non è più attivo oppure se si verificano dei problemi, è possibile rimuovere l'account mentre si risolve il problema.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Account Web mail**.

3 Selezionare l'account da rimuovere, quindi fare clic su **Rimuovi**.

Informazioni sugli account Web mail

Le tabelle seguenti descrivono le informazioni che occorre specificare quando si aggiungono o si modificano account Web mail.

Informazioni account

Informazioni	Descrizione
Descrizione	Descrivere l'account per proprio riferimento. È possibile digitare qualsiasi informazione in questa casella.
Indirizzo e-mail	Specificare l'indirizzo di posta elettronica associato all'account.
Tipo di account	Specificare il tipo di account di posta elettronica da aggiungere, ad esempio, POP3 Webmail o MSN/Hotmail.
Server	Specificare il nome del server di posta host dell'account. Se non si conosce il nome del server, consultare le informazioni fornite dal provider di servizi Internet (ISP).
Nome utente	Specificare il nome utente per l'account di posta elettronica. Ad esempio, se l'indirizzo di posta elettronica è *nomeutente*@hotmail.com, il nome utente sarà probabilmente *nomeutente*.
Password	Specificare la password per l'account di posta elettronica.
Conferma password	Verificare la password per l'account di posta elettronica.

Opzioni di controllo

Opzione	Descrizione
Controlla ogni	Anti-Spam esegue il controllo per la posta indesiderata nell'account secondo l'intervallo (numero di minuti) specificato. L'intervallo deve essere compreso tra 5 e 3600 minuti.
Controlla all'avvio	Anti-Spam controlla l'account ad ogni riavvio del computer.

Opzioni di connessione

Opzione	Descrizione
Non stabilire mai una connessione	Poiché Anti-Spam non stabilisce una connessione in modo automatico, è necessario che l'utente avvii manualmente la connessione remota.
Stabilisci una connessione quando non ne è disponibile una	Quando non è disponibile alcuna connessione a Internet, Anti-Spam tenta di connettersi mediante la connessione remota specificata dall'utente.
Utilizza sempre la connessione specificata	Anti-Spam tenta di connettersi utilizzando la connessione remota specificata dall'utente. Se attualmente si è connessi tramite una connessione remota diversa da quella specificata, la connessione verrà interrotta.
Stabilisci connessione	Specificare la connessione remota utilizzata da Anti-Spam per collegarsi a Internet.
Non interrompere la connessione al completamento del filtro	Il computer rimane connesso a Internet al termine del filtraggio.

CAPITOLO 28

Utilizzo della posta elettronica filtrata

Saltuariamente la posta indesiderata potrebbe non essere rilevata. In questo caso, è possibile segnalare la posta indesiderata a McAfee affinché possa analizzarla per creare aggiornamenti dei filtri.

Se si utilizza un account Web mail, è possibile visualizzare, esportare ed eliminare i messaggi di posta elettronica filtrati. Queste operazioni risultano utili quando non si è certi se un messaggio autorizzato è stato filtrato o se si desidera sapere quando il messaggio è stato filtrato.

In questo capitolo

Come segnalare i messaggi di posta elettronica a McAfee

È possibile segnalare i messaggi di posta elettronica a McAfee quando vengono contrassegnati come posta indesiderata o autorizzata per consentirne l'analisi e creare aggiornamenti dei filtri.

1 Aprire il riquadro Protezione da posta indesiderata.

In che modo?

1. Nel riquadro SecurityCenter fare clic su **Posta elettronica e MI**.
2. Nell'area informativa Posta elettronica e MI, fare clic su **Configura**.
3. Nel riquadro di configurazione Posta elettronica e MI, in **Protezione da posta indesiderata**, fare clic su **Avanzate**.

2 Nel riquadro Protezione da posta indesiderata, fare clic su **Barre degli strumenti posta elettronica**.

3 In **Contribuisci a migliorare Anti-Spam** selezionare le caselle di controllo appropriate, quindi fare clic su **OK**.

Per...	Procedere come segue...
Segnalare un messaggio di posta elettronica a McAfee ogni volta che viene contrassegnato come indesiderato	Selezionare **Si contrassegna il messaggio di posta elettronica come indesiderato**.
Segnalare un messaggio di posta elettronica a McAfee ogni volta che viene contrassegnato come non indesiderato	Selezionare **Si contrassegna il messaggio di posta elettronica come non indesiderato**.
Inviare l'intero messaggio di posta elettronica, non solo l'intestazione, a McAfee quando si segnala un messaggio di posta elettronica come non indesiderato.	Selezionare **Invia l'intero messaggio di posta elettronica (non solo l'intestazione)**.

Nota: quando si segnala un messaggio di posta elettronica come non indesiderato e si invia l'intero messaggio a McAfee, il messaggio non viene crittografato.

Come visualizzare, esportare o eliminare i messaggi Web mail filtrati

È possibile visualizzare, esportare o eliminare i messaggi filtrati nell'account Web mail.

1. Nella sezione **Attività comuni**, fare clic su **Rapporti e registri**.
2. Nel riquadro Rapporti e registri, fare clic su **Web mail filtrata**.
3. Selezionare un messaggio.
4. In **Desidero**, effettuare una delle seguenti operazioni:
   - Fare clic su **Visualizza** per visualizzare il messaggio nel programma di posta elettronica predefinito.
   - Fare clic su **Esporta** per copiare il messaggio nel computer.
   - Fare clic su **Elimina** per eliminare il messaggio.

Come visualizzare un evento per i messaggi Web mail filtrati

È possibile visualizzare la data e l'ora in cui i messaggi di posta elettronica sono stati filtrati e l'account che li ha ricevuti.

1. In **Attività comuni** fare clic su **Visualizza eventi recenti**.
2. Nel riquadro Eventi recenti, fare clic su **Visualizza registro**.
3. Nel riquadro sinistro, espandere l'elenco **Posta elettronica e MI**, quindi fare clic su **Eventi filtro Web mail**.
4. Selezionare il registro da visualizzare.

CAPITOLO 29

Configurazione della protezione da phishing

Anti-Spam classifica i messaggi di posta elettronica non richiesti come posta indesiderata (se invitano all'acquisto) o come phishing (se richiedono di fornire informazioni personali a siti Web notoriamente o potenzialmente fraudolenti). La protezione dal phishing protegge dall'accesso a siti Web fraudolenti. Se all'interno di un messaggio di posta elettronica si fa clic su un collegamento a un sito Web notoriamente o potenzialmente fraudolento, si viene reindirizzati alla pagina del filtro antiphishing.

Se non si desidera filtrare determinati siti Web, aggiungerli all'elenco indirizzi attendibili. È inoltre possibile modificare o rimuovere i siti Web dall'elenco indirizzi attendibili. Non è necessario aggiungere siti quali Google®, Yahoo o McAfee, in quanto tali siti non sono considerati fraudolenti.

Nota: se è installato SiteAdvisor, non si riceve la protezione dal phishing di Anti-Spam perché SiteAdvisor dispone già di una protezione dal phishing analoga a quella di Anti-Spam.

In questo capitolo

Come aggiungere un sito Web all'elenco indirizzi attendibili

Se non si desidera filtrare determinati siti Web, aggiungerli all'elenco indirizzi attendibili.

1 Aprire il riquadro Protezione da phishing.

  In che modo?

  1. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
  2. Nell'area di informazioni su Internet e rete, fare clic su **Configura**.

2 Nel riquadro Protezione da phishing fare clic su **Avanzate**.

3 In **Elenco indirizzi attendibili** fare clic su **Aggiungi**.

4 Digitare l'indirizzo del sito Web, quindi fare clic su **OK**.

Come modificare i siti dell'elenco indirizzi attendibili

Se è stato aggiunto un sito Web all'elenco indirizzi attendibili e l'indirizzo è cambiato, è possibile modificarlo.

1 Aprire il riquadro Protezione da phishing.

  In che modo?

  1. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
  2. Nell'area di informazioni su Internet e rete, fare clic su **Configura**.

2 Nel riquadro Protezione da phishing fare clic su **Avanzate**.

3 In **Elenco indirizzi attendibili**, selezionare il sito Web che si desidera aggiornare, quindi fare clic su **Modifica**.

4 Modificare il sito Web, quindi fare clic su **OK**.

Come rimuovere un sito Web dall'elenco indirizzi attendibili

Se è stato aggiunto un sito Web all'elenco indirizzi attendibili perché si desiderava accedervi, ma ora si preferisce filtrarlo, rimuoverlo dall'elenco indirizzi attendibili.

1 Aprire il riquadro Protezione da phishing.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   2. Nell'area di informazioni su Internet e rete, fare clic su **Configura**.

2 Nel riquadro Protezione da phishing fare clic su **Avanzate**.

3 In **Elenco indirizzi attendibili**, selezionare il sito Web che si desidera rimuovere, quindi fare clic su **Rimuovi**.

Come disattivare la protezione da phishing

Se si dispone già di software di protezione da phishing non di McAfee e si verifica un conflitto, è possibile disattivare la protezione da phishing di Anti-Spam.

1 Nel riquadro SecurityCenter, fare clic su **Internet e rete**.

2 Nell'area di informazioni su Internet e rete, fare clic su **Configura**.

3 In **Protezione da phishing attivata**, fare clic su **Disattiva**.

Suggerimento: al termine, ricordare di fare clic su **Attiva** in **Protezione da phishing disattivata** in modo da essere protetti dai siti Web fraudolenti.

CAPITOLO 30

McAfee Parental Controls

Il controllo genitori offre una protezione avanzata per gli utenti privati, le loro famiglie, i loro file personali e il loro computer. Consente di proteggersi dai furti di identità in linea, di bloccare la trasmissione dei dati personali e di filtrare i contenuti in linea potenzialmente offensivi (comprese le immagini). Consente inoltre di monitorare, controllare e registrare eventuali abitudini di navigazione non autorizzate e offre un'area di memorizzazione protetta per le password personali.

Prima di iniziare a utilizzare il controllo genitori, è opportuno acquisire dimestichezza con alcune delle sue funzioni più comuni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di Parental Controls.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Parental Controls

Controllo genitori	Consente di filtrare le immagini potenzialmente inappropriate, di attivare la ricerca adatta all'età, di configurare l'età dell'utente (che determina quali contenuti verranno bloccati) nonché di impostare i limiti di tempo per la navigazione sul Web (i giorni e gli orari durante i quali un utente può accedere al Web) per gli utenti di SecurityCenter. Il controllo genitori consente inoltre di limitare l'accesso a siti Web specifici da parte di tutti gli utenti e di consentire o bloccare l'accesso in base a parole chiave.
Protezione dei dati personali	Consente di bloccare la trasmissione di informazioni riservate (ad esempio, numeri di carte di credito o di conto corrente, indirizzi e così via) su Internet.
Archivio protetto password	Consente di memorizzare le password personali in modo sicuro per impedire che altri utenti, compreso un amministratore, possano accedervi.

CAPITOLO 31

Tutela dei minori

Se il computer viene utilizzato da minori, il controllo genitori consente di stabilire che cosa possono vedere e fare i minori mentre navigano sul Web. Ad esempio, è possibile attivare o disattivare la ricerca adatta all'età e il filtro delle immagini, scegliere un gruppo di classificazioni dei contenuti e definire i limiti temporali per la navigazione sul Web.

La ricerca adatta all'età assicura l'attivazione dei filtri di protezione per i motori di ricerca più diffusi, escludendo automaticamente i risultati di ricerca potenzialmente inappropriati; il filtro delle immagini blocca la visualizzazione delle immagini potenzialmente inappropriate durante la navigazione sul Web; il gruppo di classificazioni dei contenuti consente di determinare il tipo di contenuto e di siti Web cui i minori possono accedere, in base al gruppo di età. Infine i limiti temporali per la navigazione sul Web definiscono i giorni e le ore in cui i minori possono accedere al Web. È anche possibile filtrare, ossia bloccare o consentire, determinati siti Web per tutti i minori.

Nota: per configurare il controllo genitori in modo da proteggere i minori, è necessario accedere al computer come amministratore di Windows. Se è stato eseguito l'aggiornamento da una versione precedente di questo prodotto McAfee e si continua a utilizzare utenti McAfee, assicurarsi inoltre di aver effettuato l'accesso come amministratore McAfee.

In questo capitolo

Filtraggio dei siti Web mediante parole chiave

Il filtraggio con parole chiave consente di impedire agli utenti non adulti di visitare i siti Web che contengono parole potenzialmente inappropriate. Se il filtraggio con parole chiave è attivato, è disponibile un elenco di parole chiave con le regole corrispondenti che consente di classificare il contenuto in base al gruppo di classificazione. Gli utenti devono appartenere a un determinato gruppo per accedere ai siti Web che contengono parole chiave specifiche. Ad esempio, solo i membri del gruppo di utenti adulti possono visitare i siti Web contenenti la parola *porno* e solo i membri del gruppo 6-9 anni (e di età superiore) possono visitare i siti Web contenenti la parola *medicinali*.

È inoltre possibile aggiungere parole chiave consentite personalizzate all'elenco predefinito e associarle a determinati gruppi di classificazione del contenuto. Le regole associate alle parole chiave aggiunte dall'amministratore sostituiranno le regole eventualmente già associate a una corrispondente parola chiave presente nell'elenco predefinito.

Come bloccare i siti Web in base a parole chiave

Se si desidera bloccare dei siti Web a causa del contenuto inappropriato ma non si conoscono gli indirizzi specifici dei siti, è possibile bloccare i siti in base alle relative parole chiave. È sufficiente immettere una parola chiave e quindi determinare a quali gruppi di classificazione del contenuto è consentito o vietato visualizzare i siti Web che la contengono.

1 Aprire il riquadro Controllo genitori.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori fare clic su **Parole chiave** e accertarsi che sia attivato il filtraggio con parole chiave.

3 In **Elenco parole chiave**, digitare una parola chiave nella casella **Cerca**.

4 Spostare il dispositivo di scorrimento accanto a **Età minima** in modo da specificare il gruppo di età minima.
Gli utenti di età uguale o maggiore di quella specificata in questo gruppo potranno visitare i siti Web contenenti la parola chiave.

5 Fare clic su **OK**.

Come disattivare il filtraggio con parole chiave

Per impostazione predefinita, il filtraggio con parole chiave è attivato e quindi è disponibile un elenco di parole chiave con le regole corrispondenti per consentire la classificazione dei contenuti in base al gruppo di classificazione degli utenti. Sebbene McAfee lo sconsigli, è possibile disattivare il filtraggio con parole chiave in qualsiasi momento.

1 Aprire il riquadro Controllo genitori.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori, fare clic su **Parole chiave**.

3 Nel riquadro Parole chiave, fare clic su **Disattiva**.

4 Fare clic su **OK**.

Filtraggio dei siti Web

È possibile filtrare (bloccare o autorizzare) i siti Web per tutti gli utenti eccetto quelli che appartengono al gruppo degli utenti maggiori di 18 anni. Un sito Web viene bloccato per impedire ai minori di accedervi quando navigano sul Web. Se un minore prova ad accedere a un sito Web bloccato, un messaggio indica che non è possibile accedere al sito perché è stato bloccato da McAfee.

Un sito Web viene autorizzato se è stato bloccato da McAfee per impostazione predefinita ma si desidera che i minori possano accedervi. Per ulteriori informazioni sui siti Web bloccati da McAfee per impostazione predefinita, vedere Filtraggio dei siti Web mediante parole chiave (pagina 162). È inoltre possibile aggiornare o rimuovere un sito Web filtrato in qualsiasi momento.

Nota: gli utenti appartenenti al gruppo degli utenti maggiori di 18 anni, compresi gli amministratori, possono accedere a tutti i siti Web, anche a quelli bloccati. Per verificare i siti Web bloccati, è necessario effettuare l'accesso come utenti minori di 18 anni: ricordarsi però di cancellare la cronologia del browser al termine delle verifiche.

Come rimuovere un sito Web filtrato

È possibile rimuovere un sito Web filtrato se non si desidera più bloccarlo o autorizzarlo.

1 Aprire il riquadro Controllo genitori.

  In che modo?

  1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
  2. Nel riquadro Controllo genitori, fare clic su **Configura**.
  3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori, fare clic su **Siti Web filtrati**.

3 Nel riquadro Siti Web filtrati, fare clic su una voce dell'elenco **Siti Web filtrati**, quindi fare clic su **Rimuovi**.

4 Fare clic su **OK**.

Come aggiornare un sito Web filtrato

Se l'indirizzo di un sito Web cambia o viene immesso in modo non corretto quando il sito viene bloccato o autorizzato, è possibile aggiornarlo.

1 Aprire il riquadro Controllo genitori.

In che modo?

1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
2. Nel riquadro Controllo genitori, fare clic su **Configura**.
3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori, fare clic su **Siti Web filtrati**.

3 Nel riquadro Siti Web filtrati, fare clic su una voce dell'elenco **Siti Web filtrati**, modificare l'indirizzo del sito Web nella casella **http://**, quindi fare clic su **Aggiorna**.

4 Fare clic su **OK**.

Come autorizzare un sito Web

Un sito Web viene autorizzato per accertarsi che non sia bloccato per alcun utente. Se si autorizza un sito Web bloccato da McAfee per impostazione predefinita, l'impostazione predefinita viene ignorata.

1 Aprire il riquadro Controllo genitori.

In che modo?

1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
2. Nel riquadro Controllo genitori, fare clic su **Configura**.
3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori, fare clic su **Siti Web filtrati**.

3 Nel riquadro Siti Web filtrati, digitare l'indirizzo di un sito Web nella casella **http://**, quindi fare clic su **Consenti**.

4 Fare clic su **OK**.

Suggerimento: è possibile autorizzare un sito Web precedentemente bloccato facendo clic sull'indirizzo del sito nell'elenco **Siti Web filtrati** e quindi su **Consenti**.

Come bloccare un sito Web

Un sito Web viene bloccato per impedire ai minori di accedervi quando navigano sul Web. Se un minore prova ad accedere a un sito Web bloccato, viene visualizzato un messaggio per indicare che non è possibile accedere al sito perché è stato bloccato da McAfee.

1 Aprire il riquadro Controllo genitori.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, verificare che il controllo genitori sia attivato, quindi fare clic su **Avanzate**.

2 Nel riquadro Controllo genitori, fare clic su **Siti Web filtrati**.

3 Nel riquadro Siti Web filtrati, digitare l'indirizzo di un sito Web nella casella **http://**, quindi fare clic su **Blocca**.

4 Fare clic su **OK**.

Suggerimento: è possibile bloccare un sito Web precedentemente autorizzato facendo clic sull'indirizzo del sito nell'elenco **Siti Web filtrati** e quindi su **Blocca**.

Impostazione delle limitazioni degli orari di navigazione sul Web

Per evitare l'uso irresponsabile o eccessivo di Internet, è possibile impostare limiti di tempo appropriati per la navigazione sul Web da parte dei minori. Quando la navigazione sul Web viene limitata in base a orari specifici, SecurityCenter attiva sempre le restrizioni impostate, anche quando l'utente è fuori casa.

Per impostazione predefinita, a un minore è consentito navigare sul Web durante tutte le ore del giorno e della notte, sette giorni su sette, tuttavia è possibile consentire la navigazione solo in orari specifici o impedirla completamente. Se un minore prova ad accedere al Web in un periodo di tempo vietato, un avviso lo informerà che l'accesso non è autorizzato. Se la navigazione sul Web viene impedita del tutto, il minore potrà accedere e utilizzare il computer, compresi altri programmi Internet come posta elettronica, messaggistica immediata, ftp, giochi e così via, ma non navigare sul Web.

Come impostare le limitazioni degli orari di navigazione sul Web

È possibile utilizzare la griglia dei limiti di tempo per la navigazione sul Web per consentire a un minore di navigare solo in giorni e orari specifici.

1 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.
   4. Nel riquadro Controllo genitori, fare clic su **Impostazioni utente**.

2 Nel riquadro Impostazioni utente, fare clic su un nome utente e quindi su **Modifica**.

3 Nella finestra Modifica account utente, in **Limitazioni degli orari di navigazione sul Web**, trascinare il mouse per specificare i giorni e gli orari in cui l'utente non può navigare sul Web.

4 Fare clic su **OK**.

Impostazione del gruppo di classificazione del contenuto

Un utente può appartenere a uno dei seguenti gruppi di classificazione del contenuto:

- minori di 6 anni
- 6-9 anni
- 10-13 anni
- 14-18 anni
- > 18 anni

Il controllo genitori classifica (blocca o consente) i contenuti Web in base al gruppo di appartenenza di un utente. Ciò consente di bloccare o autorizzare determinati siti Web per determinati componenti della famiglia. Ad esempio, è possibile bloccare alcuni contenuti Web per gli utenti che appartengono al gruppo minori di 6 anni e consentirli per gli utenti del gruppo 10-13 anni. Per classificare il contenuto in modo più restrittivo per un utente, è possibile consentire solo la visualizzazione dei siti Web autorizzati nell'elenco **Siti Web filtrati**. Per ulteriori informazioni, vedere Filtraggio dei siti Web (pagina 164).

Come impostare il gruppo di classificazione del contenuto per un utente

Per impostazione predefinita, un nuovo utente viene aggiunto al gruppo degli utenti maggiori di 18 anni, che consente l'accesso a tutti i contenuti Web. Successivamente è possibile adeguare la classificazione del contenuto per l'utente in base all'età e al livello di maturità.

1 Aprire il riquadro Impostazioni utente.

In che modo?

1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
2. Nel riquadro Controllo genitori, fare clic su **Configura**.
3. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.
4. Nel riquadro Controllo genitori, fare clic su **Impostazioni utente**.

2 Nel riquadro Impostazioni utente, fare clic su un nome utente e quindi su **Modifica**.

3 Nella finestra Modifica account utente, in **Classificazione del contenuto**, fare clic sul gruppo di età che si desidera assegnare all'utente.

Per impedire all'utente di accedere ai siti Web bloccati nell'elenco **Siti Web filtrati**, selezionare la casella di controllo **Questo utente può solo accedere ai siti presenti nell'elenco Siti Web autorizzati**.

4 Fare clic su **OK**.

Filtraggio di immagini Web potenzialmente inappropriate

In base all'età o al livello di maturità di un utente, è possibile filtrare (bloccare o autorizzare) le immagini potenzialmente inappropriate quando l'utente naviga sul Web. Ad esempio, è possibile bloccare la visualizzazione di immagini potenzialmente inappropriate mentre un bambino sta navigando sul Web e consentirla quando l'accesso è eseguito da adolescenti e adulti. Per impostazione predefinita, il filtraggio delle immagini è disattivato per tutti i membri del gruppo degli utenti adulti e quindi eventuali immagini potenzialmente inappropriate sono visibili quando tali utenti navigano sul Web. Per ulteriori informazioni sull'impostazione di un gruppo di età per gli utenti, vedere Impostazione del gruppo di classificazione del contenuto (pagina 168).

Come filtrare immagini Web potenzialmente inappropriate

Per impostazione predefinita, i nuovi utenti vengono aggiunti al gruppo degli utenti adulti e il filtraggio delle immagini è disattivato. Se si desidera bloccare la visualizzazione di immagini potenzialmente inappropriate quando un determinato utente accede al Web, è possibile attivare il filtraggio delle immagini. Ogni immagine Web potenzialmente inappropriata viene automaticamente sostituita da un'immagine statica McAfee.

1 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.
   4. Nel riquadro Controllo genitori, fare clic su **Impostazioni utente**.

2 Nel riquadro Impostazioni utente, fare clic su un nome utente e quindi su **Modifica**.

3 Nella finestra Modifica account utente, in **Filtraggio immagini**, fare clic su **Attiva**.

4 Fare clic su **OK**.

Attivazione della ricerca adatta all'età

I motori di ricerca più diffusi (come Yahoo! e Google) offrono un'impostazione di "ricerca sicura" che impedisce la visualizzazione di risultati di ricerca potenzialmente inappropriati nell'elenco dei risultati. Di norma, tali motori di ricerca consentono di selezionare il livello del filtro di ricerca sicura, ma consentono anche a tutti gli utenti di disattivarlo in qualunque momento.

In Parental Controls, la ricerca adatta all'età consente di accertare praticamente che l'impostazione di "ricerca sicura" per un determinato utente sia sempre attiva quando si utilizzano i seguenti motori di ricerca:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Se si attiva la ricerca adatta all'età, McAfee si accerta che il filtro di ricerca sicura per il motore di ricerca sia attivo per tale utente e impostato sul livello più restrittivo. Inoltre, se un utente tenta di disattivarlo (nelle preferenze del motore di ricerca o nelle impostazioni avanzate), McAfee lo riattiverà automaticamente.

Per impostazione predefinita, la ricerca adatta all'età è attivata per tutti gli utenti, eccetto l'amministratore e gli utenti del gruppo di età > 18 anni. Per ulteriori informazioni sull'impostazione di un gruppo di età per gli utenti, vedere Impostazione del gruppo di classificazione del contenuto (pagina 168).

Come attivare la ricerca adatta all'età

Per impostazione predefinita, i nuovi utenti vengono aggiunti al gruppo degli utenti maggiori di 18 anni e la funzionalità di ricerca adatta all'età è disattivata. Se si desidera che il filtro per le ricerche sicure offerto dai motori di ricerca più diffusi sia attivato per gli utenti maggiori di 18 anni, è possibile attivare tale funzionalità.

1 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   2. Nel riquadro Controllo genitori, fare clic su **Configura**.
   3. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.
   4. Nel riquadro Controllo genitori, fare clic su **Impostazioni utente**.

2 Nel riquadro Impostazioni utente, fare clic su un nome utente e quindi su **Modifica**.

3 Nella finestra Modifica account utente, in **Ricerca adatta all'età**, fare clic su **Attiva**.

4 Fare clic su **OK**.

CAPITOLO 32

Configurazione degli utenti

Per configurare il controllo genitori per la protezione dei minori, si assegnano determinate autorizzazioni ai minori in SecurityCenter. Tali autorizzazioni determinano che cosa possono vedere e fare i minori mentre navigano sul Web.

Per impostazione predefinita, gli utenti SecurityCenter corrispondono agli utenti Windows impostati sul computer. Tuttavia, se si esegue un aggiornamento da una versione precedente di SecurityCenter che utilizzava utenti McAfee, verranno mantenuti gli utenti McAfee con le relative autorizzazioni.

Nota: per configurare gli utenti, è necessario accedere al computer come amministratore di Windows. Se è stato eseguito l'aggiornamento da una versione precedente di questo prodotto McAfee e si continua a utilizzare utenti McAfee, assicurarsi inoltre di aver effettuato l'accesso come amministratore McAfee.

In questo capitolo

Utilizzo degli utenti McAfee

Se è stato eseguito un aggiornamento da una versione precedente di SecurityCenter che utilizzava utenti McAfee, verranno automaticamente mantenuti gli utenti McAfee con le relative autorizzazioni. È possibile continuare a configurare e gestire gli utenti McAfee, tuttavia è consigliabile passare agli utenti Windows. Una volta eseguito il passaggio agli utenti Windows, non sarà più possibile ritornare agli utenti McAfee.

Se si continua ad utilizzare utenti McAfee, sarà possibile aggiungere, modificare o rimuovere gli utenti e modificare o ripristinare la password dell'amministratore McAfee.

Come recuperare la password dell'amministratore McAfee

Se si dimentica la password di amministratore, è possibile recuperarla.

1 Fare clic con il pulsante destro del mouse sull'icona di SecurityCenter, quindi fare clic su **Cambia utente**.

2 Nell'elenco **Nome utente**, fare clic su **Amministratore**, quindi su **Password dimenticata**.

3 Digitare la risposta alla domanda segreta nella casella **Risposta**.

4 Fare clic su **Invia**.

Come modificare la password dell'amministratore McAfee

È possibile modificare la password dell'amministratore McAfee nel caso in cui sia difficile da ricordare o si ritenga che possa essere compromessa.

1 Accedere a SecurityCenter come amministratore.

2 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   3. Nel riquadro Controllo genitori, fare clic su **Configura**.
   4. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.

3 Nel riquadro Impostazioni utente, in **Account utente McAfee**, selezionare **Amministratore** e fare clic su **Modifica**.

4 Nella finestra di dialogo Modifica account utente, digitare una nuova password nella casella **Nuova password**, quindi digitarla di nuovo nella casella **Immettere nuovamente la password**.

5 Fare clic su **OK**.

Come rimuovere un utente McAfee

È possibile rimuovere un utente McAfee in qualsiasi momento.

Per rimuovere un utente McAfee:

1 Accedere a SecurityCenter come amministratore.

2 Aprire il riquadro Impostazioni utente.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
3. Nel riquadro Controllo genitori, fare clic su **Configura**.
4. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.

3 Nel riquadro Impostazioni utente, in **Account utente McAfee**, selezionare un nome utente e fare clic su **Rimuovi**.

Come modificare i dati di un account utente McAfee

È possibile modificare la password, il tipo di account o la funzione di accesso automatico per un utente McAfee.

1 Accedere a SecurityCenter come amministratore.

2 Aprire il riquadro Impostazioni utente.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
3. Nel riquadro Controllo genitori, fare clic su **Configura**.
4. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.

3 Nel riquadro Impostazioni utente, fare clic su un nome utente e quindi su **Modifica**.

4 Seguire le istruzioni visualizzate sullo schermo per modificare la password, il tipo di account o la protezione del controllo genitori relativi all'utente.

5 Fare clic su **OK**.

Come aggiungere un utente McAfee

Dopo avere creato un utente McAfee, è possibile configurare la protezione del controllo genitori per quell'utente. Per ulteriori informazioni, consultare la Guida in linea di Parental Controls.

1 Accedere a SecurityCenter come amministratore.

2 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   3. Nel riquadro Controllo genitori, fare clic su **Configura**.
   4. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.

3 Nel riquadro Impostazioni utente, fare clic su **Aggiungi**.

4 Seguire le istruzioni visualizzate sullo schermo per impostare il nome utente, la password, il tipo di account e la protezione del controllo genitori.

5 Fare clic su **Crea**.

Come passare agli utenti Windows

Per semplificare la gestione, si consiglia di passare agli utenti Windows; tuttavia, in tal caso, non sarà più possibile ritornare agli utenti McAfee.

1 Aprire il riquadro Impostazioni utente.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Controllo genitori**.
   3. Nel riquadro Controllo genitori, fare clic su **Configura**.
   4. Nel riquadro di configurazione Controllo genitori, fare clic su **Avanzate**.

2 Nel riquadro Impostazioni utente, fare clic su **Passa a**.

3 Confermare l'operazione.

Utilizzo degli utenti Windows

Per impostazione predefinita, gli utenti SecurityCenter corrispondono agli utenti Windows impostati sul computer. Le operazioni di aggiunta di un utente, modifica delle informazioni sull'account utente o rimozione di un utente vengono eseguite nella console Gestione computer di Windows. Sarà quindi possibile impostare la protezione del controllo genitori per tali utenti in SecurityCenter.

Se è stato effettuato un aggiornamento da una versione precedente di SecurityCenter che utilizzava utenti McAfee, consultare Utilizzo degli utenti McAfee (pagina 174).

CAPITOLO 33

Protezione delle informazioni sul Web

È possibile impedire la trasmissione via Web di dati personali (come nome, indirizzo, numeri della carta di credito e del conto bancario) aggiungendoli all'area dei dati protetti.

Nota: il controllo genitori non blocca la trasmissione delle informazioni personali da parte dei siti Web protetti (ossia i siti Web che utilizzano il protocollo https://), quali i siti di servizi bancari.

In questo capitolo

Protezione delle informazioni personali

È possibile bloccare i dati personali, come nome, indirizzo, numeri della carta di credito e del conto bancario, per impedirne la trasmissione sul Web. Se McAfee rileva dati personali contenuti in un oggetto, ad esempio il campo di un modulo o un file, che sta per essere inviato sul Web, si verifica quanto segue:

- L'amministratore deve confermare se inviare o meno le informazioni.
- Per gli altri utenti, la porzione bloccata viene sostituita da asterischi (*). Ad esempio, se un sito Web dannoso tenta di inviare il numero di carta di credito dell'utente a un altro computer, tale numero viene sostituito da asterischi.

Come proteggere le informazioni personali

È possibile bloccare i seguenti tipi di dati personali: nome, indirizzo, CAP, codice fiscale, numero di telefono, numeri di carta di credito, conti bancari, conti titoli e schede telefoniche. Per bloccare dati personali di tipo diverso è possibile impostare il tipo su **altro**.

1 Aprire il riquadro Dati protetti.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro di configurazione Internet e rete, verificare che la protezione dei dati personali sia attivata, quindi fare clic su **Avanzate**.

2 Nel riquadro Dati protetti, fare clic su **Aggiungi**.

3 Selezionare dall'elenco il tipo di dati che si desidera bloccare.

4 Immettere i dati personali, quindi fare clic su **OK**.

CAPITOLO 34

Protezione delle password

L'archivio protetto password è un'area di memorizzazione protetta per le password personali. Consente di memorizzare le password in modo sicuro per impedire che altri utenti, compreso un amministratore, possano accedervi.

In questo capitolo

Impostazione dell'archivio protetto password

Prima di iniziare a utilizzare l'archivio protetto password è necessario impostare la relativa password. Solo gli utenti che conoscono questa password possono accedere all'archivio protetto password. Se la password viene dimenticata è possibile reimpostarla; tuttavia, tutte le password precedentemente memorizzate nell'archivio protetto password verranno eliminate.

Dopo aver impostato una password per l'archivio protetto è possibile aggiungere, modificare o rimuovere password dall'archivio. È inoltre possibile modificare la password dell'archivio protetto in qualsiasi momento.

Come reimpostare la password dell'archivio protetto

Se la password dell'archivio protetto viene dimenticata è possibile reimpostarla; tuttavia, tutte le password precedentemente immesse verranno eliminate.

1 Aprire il riquadro Archivio protetto password.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate** nella sezione **Archivio protetto password**.

2 Fare clic su **Password dimenticata?**

3 Nella finestra di dialogo Reimposta archivio protetto, digitare una nuova password nella casella **Password**, quindi digitarla di nuovo nella casella **Immettere nuovamente la password**.

4 Fare clic su **Reimposta**.

5 Nella finestra di dialogo Conferma reimpostazione password, fare clic su **Sì**.

Come modificare la password dell'archivio protetto

È possibile modificare la password dell'archivio protetto in qualsiasi momento.

1 Aprire il riquadro Archivio protetto password.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate** nella sezione **Archivio protetto password**.

2 Nel riquadro Archivio protetto password, digitare la password corrente nella casella **Password**, quindi fare clic su **Apri**.

3 Nel riquadro Gestisci archivio protetto password, fare clic su **Modifica password**.

4 Digitare una nuova password nella casella **Scegliere la password** e digitarla nuovamente nella casella **Immettere nuovamente la password**.

5 Fare clic su **OK**.

6 Nella finestra di dialogo Password dell'archivio protetto password modificata, fare clic su **OK**.

Come rimuovere una password

È possibile rimuovere una password dall'archivio protetto in qualsiasi momento. Non è possibile recuperare una password rimossa dall'archivio.

1 Aprire il riquadro Archivio protetto password.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate** nella sezione **Archivio protetto password**.

2 Digitare la password dell'archivio protetto nella casella **Password**.

3 Fare clic su **Apri**.

4 Nel riquadro Gestisci archivio protetto password, fare clic su una password, quindi su **Rimuovi**.

5 Nella finestra di dialogo Conferma rimozione, fare clic su **Sì**.

Come modificare una password

Per garantire che le voci dell'archivio protetto password siano sempre precise e affidabili è necessario aggiornarle in corrispondenza della modifica delle password.

1 Aprire il riquadro Archivio protetto password.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate** nella sezione **Archivio protetto password**.

2 Digitare la password dell'archivio protetto nella casella **Password**.

3 Fare clic su **Apri**.

4 Nel riquadro Gestisci archivio protetto password, fare clic su una password, quindi su **Modifica**.

5 Modificare la descrizione della password (ad esempio, il suo scopo) nella casella **Descrizione** oppure modificare la password nella casella **Password**.

6 Fare clic su **OK**.

Come aggiungere una password

Se si hanno difficoltà nel tenere a mente le proprie password, è possibile aggiungerle all'archivio protetto. L'archivio protetto password è un'area protetta a cui possono accedere solo gli utenti che ne conoscono la password.

1 Aprire il riquadro Archivio protetto password.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro SecurityCenter, fare clic su **Internet e rete**.
   3. Nella sezione Internet e rete, fare clic su **Configura**.
   4. Nel riquadro Configurazione di Internet e rete, fare clic su **Avanzate** nella sezione **Archivio protetto password**.

2 Digitare la password dell'archivio protetto nella casella **Password**.

3 Fare clic su **Apri**.

4 Nel riquadro Gestisci archivio protetto password, fare clic su **Aggiungi**.

5 Digitare una descrizione della password (ad esempio, il suo scopo) nella casella **Descrizione**, quindi digitare la password nella casella **Password**.

6 Fare clic su **OK**.

CAPITOLO 35

McAfee Backup and Restore

Utilizzare McAfee® Backup and Restore per prevenire perdite accidentali di dati archiviando i file su CD, DVD, unità USB, disco rigido esterno o unità di rete. Con l'archiviazione locale è possibile memorizzare i file personali in CD, DVD, unità USB, dischi rigidi esterni o unità di rete. In tal modo si conserva una copia locale di record, documenti e altro materiale importante in caso di perdite dei dati accidentali.

Prima di iniziare a utilizzare Backup and Restore, è opportuno acquisire dimestichezza con alcune delle funzioni più comuni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di Backup and Restore. Dopo aver esaminato le funzionalità del programma, sarà necessario verificare la disponibilità di supporti di memorizzazione adeguati per la creazione di archivi locali.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Backup and Restore

Archiviazione locale pianificata	È possibile proteggere i dati archiviando file e cartelle in CD, DVD, unità USB, disco rigido esterno o unità di rete. Una volta avviato il primo archivio, l'esecuzione di quelli incrementali avverrà automaticamente.
Ripristino con un solo clic	Nel caso in cui file e cartelle vengano erroneamente eliminati o risultino danneggiati sul computer, sarà possibile ripristinare le versioni archiviate più recentemente dai supporti di archiviazione utilizzati.
Compressione e crittografia	Per impostazione predefinita, i file archiviati vengono compressi in modo da occupare meno spazio nei supporti di archiviazione. Come ulteriore misura di protezione, gli archivi vengono crittografati per impostazione predefinita.

CAPITOLO 36

Archiviazione di file

È possibile utilizzare McAfee Backup and Restore per archiviare su CD, DVD, unità USB, disco rigido esterno o unità di rete una copia dei file residenti sul computer. L'archiviazione dei file consente di ripristinare facilmente le informazioni in caso di perdite o danni accidentali ai dati.

Prima di iniziare ad archiviare i file, è necessario selezionare il percorso di archiviazione predefinito (CD, DVD, unità USB, disco rigido esterno o unità di rete). Alcune configurazioni in McAfee sono preimpostate, ad esempio le cartelle e i tipi di file da archiviare, ma è possibile modificarle.

Dopo aver impostato le opzioni di archiviazione locale, sarà possibile modificare le impostazioni predefinite relative alla frequenza con cui Backup and Restore dovrà eseguire archiviazioni complete o rapide. È possibile eseguire archiviazioni manuali in qualsiasi momento.

In questo capitolo

Attivazione e disattivazione dell'archivio locale

La prima volta che viene avviato Backup and Restore, si determina se attivare o disattivare l'archivio locale, in base alla modalità di utilizzo desiderata per Backup and Restore. Dopo aver eseguito l'accesso e aver iniziato a utilizzare Backup and Restore, è possibile attivare o disattivare l'archiviazione locale in qualsiasi momento.

Se non si desidera archiviare una copia dei file residenti nel computer su CD, DVD, unità USB, disco rigido esterno o unità di rete, è possibile disattivare l'archivio locale.

Come attivare l'archivio locale

Attivare l'archivio locale se si desidera archiviare una copia dei file residenti sul computer su CD, DVD, unità USB, disco rigido esterno o unità di rete.

1 Nel **Menu avanzato** di SecurityCenter fare clic su **Configura**.
2 Nel riquadro Configura, fare clic su **Computer e file**.
3 Nel riquadro di configurazione Computer e file, in **L'archivio locale è disabilitato**, fare clic su **Attiva**.

Come disattivare l'archivio locale

Disattivare l'archivio locale se non si desidera archiviare una copia dei file residenti sul computer su CD, DVD, unità USB, disco rigido esterno o unità di rete.

1 Nel **Menu avanzato** di SecurityCenter fare clic su **Configura**.
2 Nel riquadro Configura, fare clic su **Computer e file**.
3 Nel riquadro di configurazione Computer e file, in **L'archivio locale è abilitato**, fare clic su **Disattiva**.

Impostazione delle opzioni di archiviazione

Prima di iniziare ad archiviare i file, è necessario impostare alcune opzioni di archiviazione locale. È, ad esempio, necessario impostare i percorsi e i tipi di file monitorati. I percorsi di monitoraggio sono cartelle all'interno del computer tenute sotto controllo da Backup and Restore per il rilevamento di nuovi file o di modifiche ai file esistenti. I file monitorati sono i tipi di file (ad esempio DOC, XLS e così via) che in Backup and Restore vengono memorizzati negli archivi all'interno dei percorsi di monitoraggio. Per impostazione predefinita, viene eseguita l'archiviazione dei tipi di file riportati di seguito. È tuttavia possibile archiviare anche altri tipi di file.

- Documenti di Microsoft® Word (DOC, DOCX)
- Fogli di calcolo di Microsoft Excel® (XLS, XLSX)
- Presentazioni di Microsoft PowerPoint® (PPT, PPTX)
- File di Microsoft Project® (MPP)
- File PDF di Adobe® (PDF)
- File di testo (TXT)
- File HTML (HTML)
- File Joint Photographic Experts Group (JPG, JPEG)
- File Tagged Image Format (TIF)
- File MPEG Audio Stream III (MP3)
- File video (VDO)

Nota: non è possibile archiviare i seguenti tipi di file: OST e PST.

È possibile impostare due tipi di percorso di monitoraggio: cartelle e sottocartelle di livello superiore o solo cartelle di livello superiore. Se si imposta un percorso di cartelle e sottocartelle di livello superiore, in Backup and Restore verranno archiviati i tipi di file monitorati in quella cartella e nelle relative sottocartelle. Se si imposta il percorso di cartelle di livello superiore, in Backup and Restore verranno archiviati i tipi di file monitorati solo nella cartella (e non nelle relative sottocartelle). È possibile inoltre identificare i percorsi che si desidera escludere dall'archiviazione locale. Per impostazione predefinita, Desktop e Documenti di Windows sono impostati come percorsi di monitoraggio di cartelle e sottocartelle di livello superiore.

Dopo aver impostato i tipi di file monitorati e i relativi percorsi, sarà necessario impostare il percorso di archiviazione, ovvero CD, DVD, unità USB, disco rigido esterno o unità di rete in cui verranno memorizzati i dati archiviati. È possibile modificare il percorso di archiviazione in qualsiasi momento.

Per motivi di sicurezza o per risolvere i problemi correlati alle dimensioni degli archivi, la crittografia o la compressione sono attivate per impostazione predefinita per i file archiviati. I file crittografati vengono trasformati da testo in codice, oscurando le informazioni per renderle illeggibili agli utenti che non dispongono dei mezzi necessari per decifrarle. I file vengono compressi in un formato che consente di ridurre al minimo lo spazio necessario per la memorizzazione o la trasmissione. Sebbene McAfee lo sconsigli, è possibile disattivare la crittografia o la compressione in qualsiasi momento.

Come includere un percorso nell'archivio

È possibile impostare due tipi di percorso di monitoraggio per l'archiviazione: cartelle e sottocartelle di livello superiore o solo cartelle di livello superiore. Se si imposta un percorso di cartelle e sottocartelle di livello superiore, in Backup and Restore verranno monitorati gli eventuali cambiamenti del contenuto della cartella e delle relative sottocartelle. Se si imposta un percorso di cartelle di livello superiore, in Backup and Restore verrà monitorato il contenuto della sola cartella (non delle relative sottocartelle).

1. Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.

2. Fare clic su **Percorsi monitorati**.
3. Eseguire una delle seguenti operazioni:
   - Per archiviare il contenuto di una cartella, incluso il contenuto delle relative sottocartelle, fare clic su **Aggiungi cartella** in **Archiviazione cartelle e sottocartelle di livello superiore**.
   - Per archiviare il contenuto di una cartella, ma non il contenuto delle relative sottocartelle, fare clic su **Aggiungi cartella** in **Archiviazione cartelle di livello superiore**.
   - Per archiviare un intero file, fare clic su **Aggiungi file** in **Archiviazione cartelle di livello superiore**.
4. Nella finestra di dialogo Cerca cartella (o Apri), spostarsi nella cartella (o nel file) da monitorare e fare clic su **OK**.
5. Fare clic su **OK**.

Suggerimento: per monitorare con Backup and Restore una cartella che non è stata ancora creata, fare clic su **Crea nuova cartella** nella finestra di dialogo Cerca cartella, per aggiungere una cartella e contemporaneamente impostarla come percorso di monitoraggio.

Come impostare i tipi di file di archiviazione

È possibile specificare quali tipi di file verranno archiviati all'interno dei percorsi di cartelle e sottocartelle di livello superiore o cartelle di livello superiore. È possibile selezionare un'opzione da un elenco di tipi di file esistenti o aggiungere un nuovo tipo all'elenco.

1 Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.

2 Fare clic su **Tipi di file**.

3 Espandere gli elenchi dei tipi di file e selezionare le caselle di controllo accanto ai tipi che si desidera archiviare.

4 Fare clic su **OK**.

Suggerimento: per aggiungere un nuovo tipo di file all'elenco **Tipi di file** selezionati, digitare l'estensione del file nella casella **Aggiungi tipo file personalizzato ad Altro**, fare clic su **Aggiungi** e quindi su **OK**. Il nuovo tipo di file diventa automaticamente un file monitorato.

Come escludere un percorso dall'archivio

È possibile escludere un percorso dall'archivio per evitare che tale percorso (cartella) e il relativo contenuto vengano archiviati.

1 Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.

2 Fare clic su **Percorsi monitorati**.

3 Fare clic su **Aggiungi cartella** in **Cartelle escluse dal backup**.

4 Nella finestra di dialogo Cerca cartella, spostarsi nella cartella da escludere, selezionarla e fare clic su **OK**.

5 Fare clic su **OK**.

Suggerimento: per escludere con Backup and Restore una cartella che non è stata ancora creata, fare clic su **Crea nuova cartella** nella finestra di dialogo Cerca cartella, per aggiungere una cartella ed escluderla contemporaneamente.

Come modificare il percorso di archiviazione

Quando si modifica il percorso di archiviazione, i file archiviati in precedenza in una posizione diversa vengono elencati in *Mai archiviato*.

1 Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.

2 Fare clic su **Modifica percorso archivio**.

3 Nella finestra di dialogo Percorso archivio, effettuare una delle seguenti operazioni:

   - Fare clic su **Seleziona masterizzatore CD/DVD**, fare clic sull'unità CD o DVD nell'elenco **Masterizzatore**, quindi scegliere **OK**.
   - Fare clic su **Seleziona percorso unità**, spostarsi in un'unità USB, unità locale o disco rigido esterno, selezionare e fare clic su **OK**.
   - Fare clic su **Seleziona un percorso di rete**, spostarsi in una cartella di rete, selezionarla e fare clic su **OK**.

4 Verificare il nuovo percorso di archiviazione in **Percorso archivio selezionato** e fare clic su **OK**.

5 Nella finestra di dialogo di conferma, fare clic su **OK**.

6 Fare clic su **OK**.

Nota: quando si modifica il percorso di archiviazione, i file archiviati in precedenza vengono elencati come **Non archiviato** nella colonna **Stato**.

Come disattivare crittografia e compressione per l'archiviazione

La crittografia dei file archiviati protegge la riservatezza dei dati oscurando il contenuto dei file per renderli illeggibili. La compressione dei file archiviati consente di ridurre le dimensioni dei file. Per impostazione predefinita, sia la crittografia che la compressione sono attivate, ma è possibile disattivarle in qualsiasi momento.

1 Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.

2 Fare clic su **Impostazioni avanzate**.

3 Deselezionare la casella di controllo **Attiva la crittografia per aumentare la protezione**.

4 Deselezionare la casella di controllo **Attiva la compressione per ridurre lo spazio utilizzato**.

5 Fare clic su **OK**.

Nota: McAfee consiglia di non disattivare la crittografia e la compressione durante l'archiviazione dei file.

Esecuzione di archiviazioni complete e rapide

È possibile eseguire due tipi di archiviazione: completa o rapida. Con un'archiviazione completa, si memorizza un set completo di dati in base ai tipi di file e ai percorsi di monitoraggio impostati. Con un'archiviazione rapida, si archiviano solo i file monitorati modificati dall'ultima archiviazione completa o rapida.

Per impostazione predefinita, la pianificazione di Backup and Restore prevede un'archiviazione completa dei tipi di file monitorati presenti nei relativi percorsi ogni lunedì alle ore 9.00 e un'archiviazione rapida ogni 48 ore dall'ultima archiviazione completa o rapida. Questo tipo di pianificazione garantisce che sia sempre gestito un archivio di file corrente. Tuttavia, se non si desidera eseguire l'archiviazione ogni 48 ore, sarà possibile modificare la pianificazione secondo le proprie esigenze.

È possibile archiviare manualmente il contenuto dei percorsi di monitoraggio in qualsiasi momento. Se, ad esempio, un file viene modificato e deve essere archiviato, ma in Backup and Restore non è pianificata un'archiviazione completa o rapida nelle ore successive, sarà possibile eseguire l'archiviazione manualmente. Dopo l'archiviazione manuale dei file, l'intervallo impostato per le archiviazioni automatiche verrà reimpostato.

È inoltre possibile interrompere un'archiviazione automatica o manuale eseguita in un orario inadeguato. Se, ad esempio, si sta eseguendo un'attività che occupa molte risorse e viene avviata un'archiviazione automatica, sarà possibile arrestarla. Quando si interrompe un'archiviazione automatica, l'intervallo impostato per le archiviazioni automatiche viene reimpostato.

Come pianificare le archiviazioni automatiche

È possibile impostare la frequenza delle archiviazioni complete e rapide per assicurarsi che i dati siano sempre protetti.

1. Aprire la finestra di dialogo Impostazioni archivio locale.

   In che modo?

   1. Fare clic sulla scheda **Archivio locale**.
   2. Nel riquadro di sinistra, fare clic su **Impostazioni**.
2. Fare clic su **Generale**.
3. Per eseguire un'archiviazione completa ogni giorno, settimana o mese, fare clic su una delle seguenti voci in **Esegui archiviazione completa ogni**:
   - **Giorno**
   - **Settimana**
   - **Mese**
4. Selezionare la casella di controllo accanto al giorno in cui si desidera eseguire l'archiviazione completa.
5. Fare clic su un valore nell'elenco **Alle** per indicare l'ora in cui eseguire l'archiviazione completa.
6. Per eseguire un'archiviazione rapida con cadenza giornaliera o oraria, fare clic su una delle seguenti voci in **Archiviazione rapida**:
   - **Ore**
   - **Giorni**
7. Nella casella **Esegui archiviazione rapida ogni** digitare un numero che indica la frequenza.
8. Fare clic su **OK**.

Nota: è possibile disattivare un'archiviazione pianificata selezionando **Manuale** in **Esegui archiviazione completa ogni**.

Come interrompere un'archiviazione automatica

In Backup and Restore l'archiviazione automatica dei file e delle cartelle nei percorsi di monitoraggio viene eseguita in base alla pianificazione impostata. Tuttavia, è possibile interrompere in qualsiasi momento un'archiviazione automatica in corso.

1. Nel riquadro di sinistra, fare clic su **Interrompi archiviazione**.
2. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Nota: il collegamento **Interrompi archiviazione** viene visualizzato solo quando è in corso un'archiviazione.

Come eseguire manualmente l'archiviazione

Le archiviazioni automatiche vengono eseguite in base a una pianificazione predefinita, ma è possibile eseguire manualmente un'archiviazione rapida o completa in qualsiasi momento. Con un'archiviazione rapida si memorizzano solo i file modificati rispetto all'ultima archiviazione completa o rapida. Con un'archiviazione completa vengono memorizzati i tipi di file monitorati in tutti i percorsi di monitoraggio.

1 Fare clic sulla scheda **Archivio locale**.
2 Eseguire una delle seguenti operazioni:
   - Per eseguire un'archiviazione rapida, fare clic su **Archiviazione rapida** nel riquadro di sinistra.
   - Per eseguire un'archiviazione completa, fare clic su **Archiviazione completa** nel riquadro di sinistra.
3 Nella finestra di dialogo Avvia archiviazione, verificare lo spazio disponibile e le impostazioni, quindi scegliere **Continua**.

CAPITOLO 37

Utilizzo dei file archiviati

Dopo l'archiviazione, sarà possibile utilizzare i file con Backup and Restore. I file archiviati vengono visualizzati in una normale finestra di gestione dei file che consente di individuarli facilmente. Quando le dimensioni dell'archivio crescono, è possibile ordinare i file o eseguire delle ricerche. È possibile inoltre aprire i file direttamente nella finestra di gestione per esaminarne il contenuto senza dover ripristinare i file.

I file vengono ripristinati da un archivio se la copia locale del file risulta non aggiornata, mancante o danneggiata. In Backup and Restore sono inoltre disponibili le informazioni necessarie per gestire gli archivi locali e i supporti di memorizzazione.

In questo capitolo

Utilizzo della finestra di gestione degli archivi locali

Nella finestra di gestione degli archivi locali è possibile visualizzare e manipolare i file archiviati localmente. Per ciascun file è possibile visualizzare nome, tipo, percorso, dimensioni, stato (archiviato, non archiviato o archiviazione in corso) e data dell'ultima archiviazione. È inoltre possibile ordinare i file in base a uno di tali criteri.

Se l'archivio è ampio, è possibile trovare rapidamente un file eseguendo una ricerca. È possibile cercare l'intero nome del file o del percorso, o solo una parte, quindi limitare la ricerca indicando le dimensioni approssimative del file e la data dell'ultima archiviazione.

Dopo aver individuato un file, sarà possibile aprirlo direttamente nella finestra di gestione degli archivi locali. Backup and Restore consente di aprire il file nel programma di origine e di apportare modifiche senza chiudere la finestra di gestione. Il file viene salvato nel percorso di monitoraggio originale del computer e viene automaticamente archiviato in base alla pianificazione definita.

Ordinamento dei file archiviati

È possibile ordinare le cartelle e i file archiviati in base ai seguenti criteri: nome, tipo, dimensioni, stato (archiviato, non archiviato o archiviazione in corso), data dell'ultima archiviazione o percorso dei file nel computer.

Per ordinare file archiviati:

1 Fare clic sulla scheda **Archivio locale**.

2 Nel riquadro di destra, fare clic sul nome di una colonna.

Come cercare un file archiviato

Se l'archivio è molto ampio, è possibile trovare rapidamente un file eseguendo una ricerca. È possibile cercare l'intero nome del file o del percorso, o solo una parte, quindi limitare la ricerca indicando le dimensioni approssimative del file e la data dell'ultima archiviazione.

1 Digitare il nome, o parte di esso, del file nella casella **Cerca** nella parte superiore della schermata, quindi premere INVIO.
2 Nella casella **Percorso o parte di esso** digitare il percorso completo o una parte dello stesso.
3 Indicare le dimensioni approssimative del file che si desidera cercare, in uno dei modi seguenti:
   - Fare clic su **Meno di 100 KB**, **Meno di 1 MB** o **Più di 1 MB**.
   - Fare clic su **Dimensioni in KB**, quindi specificare nelle caselle le dimensioni appropriate.
4 Indicare la data approssimativa dell'ultima archiviazione del file, in uno dei modi seguenti:
   - Fare clic su **Settimana in corso**, **Mese in corso** oppure **Anno in corso**.
   - Fare clic su **Specifica le date**, scegliere **Archiviato** nell'elenco e selezionare le date appropriate dai relativi elenchi.
5 Fare clic su **Cerca**.

Nota: se non si conosce la dimensione o la data approssimativa dell'ultima archiviazione, fare clic su **Sconosciuto**.

Apertura di un file archiviato

È possibile esaminare il contenuto di un file archiviato aprendolo direttamente nella finestra di ricerca archivi locali.

Per aprire i file archiviati:

1 Fare clic sulla scheda **Archivio locale**.
2 Nel riquadro di destra, scegliere un nome file e fare clic su **Apri**.

Suggerimento: è possibile aprire un file archiviato anche facendo doppio clic sul nome del file.

Ripristino di file archiviati

Se un file monitorato risulta danneggiato, mancante o viene cancellato per errore, sarà possibile ripristinarne una copia da un archivio locale. Per questo motivo, è importante verificare che i file vengano archiviati con regolarità. È inoltre possibile ripristinare versioni più datate dei file da un archivio locale. Se, ad esempio, un file viene archiviato con regolarità, ma si desidera tornare a una versione precedente del file, sarà possibile individuare il file corrispondente nel percorso di archiviazione. Se il percorso di archiviazione è un'unità locale o di rete, sarà possibile eseguire la ricerca del file. Se il percorso è un disco rigido esterno o un'unità USB, sarà necessario collegare l'unità al computer, quindi eseguire la ricerca del file. Se il percorso è un CD o un DVD, sarà necessario inserire il CD o il DVD nel computer, quindi eseguire la ricerca del file.

È inoltre possibile ripristinare file archiviati in un altro computer. Se, ad esempio, un set di file viene archiviato in un disco rigido esterno del computer A, sarà possibile ripristinare i file nel computer B. Per questa operazione, è necessario installare Backup and Restore nel computer B e collegare il disco rigido esterno. Quindi, in Backup and Restore, cercare i file che verranno aggiunti all'elenco **File mancanti** per il ripristino.

Per ulteriori informazioni sull'archiviazione dei file, vedere Archiviazione di file. Se un file monitorato viene cancellato intenzionalmente dall'archivio, sarà possibile cancellarlo anche dall'elenco **File mancanti**.

Come ripristinare i file mancanti da un archivio locale

Con l'archiviazione locale di Backup and Restore è possibile ripristinare i dati mancanti da una cartella monitorata sul computer locale. Se ad esempio un file viene spostato da una cartella monitorata o viene eliminato, ed è stato già archiviato, sarà possibile ripristinarlo dall'archivio locale.

1. Fare clic sulla scheda **Archivio locale**.
2. Nella scheda **File mancanti** nella parte inferiore della schermata, selezionare la casella di controllo accanto al nome del file da ripristinare.
3. Fare clic su **Ripristina**.

Suggerimento: è possibile ripristinare tutti i file dell'elenco **File mancanti** facendo clic su **Ripristina tutto**.

Ripristino della versione precedente di un file da un archivio locale

Per ripristinare una versione precedente di un file archiviato, è possibile individuarlo e aggiungerlo all'elenco **File mancanti**. Ripristinare quindi il file, come per qualsiasi altro file presente nell'elenco **File mancanti**.

1. Fare clic sulla scheda **Archivio locale**.
2. Nella scheda **File mancanti** nella parte inferiore della schermata, fare clic su **Sfoglia** quindi spostarsi nella posizione in cui si trova l'archivio.

   I nomi delle cartelle archiviate hanno il seguente formato: `cre ggmmaa_hh-mm-ss_***`, dove `ggmmaa` è la data in cui i file sono stati archiviati, `hh-mm-ss` è l'ora in cui i file sono stati archiviati e `***` può essere `Completo o Inc`, a seconda del tipo di archivio, completo o rapido.
3. Selezionare il percorso, quindi scegliere **OK**.

   I file contenuti nel percorso selezionato verranno visualizzati nell'elenco **File mancanti**, pronti per essere ripristinati. Per ulteriori informazioni, vedere Ripristino di file mancanti da un archivio locale (pagina 202).

Rimozione di file dall'elenco dei file mancanti

Quando un file archiviato viene spostato da una cartella monitorata o eliminato, viene visualizzato automaticamente nell'elenco **File mancanti**. L'utente viene così informato che esiste un'incoerenza tra i file archiviati e quelli contenuti nelle cartelle monitorate. Se il file è stato spostato dalla cartella monitorata o è stato eliminato intenzionalmente, sarà possibile cancellarlo dall'elenco **File mancanti**.

Per rimuovere un file dall'elenco File mancanti:

1. Fare clic sulla scheda **Archivio locale**.
2. Nella scheda **File mancanti** nella parte inferiore della schermata, selezionare la casella di controllo accanto al nome del file da rimuovere.
3. Fare clic su **Elimina**.

Suggerimento: è possibile rimuovere tutti i file dell'elenco **File mancanti** facendo clic su **Elimina tutto**.

Gestione degli archivi

È possibile in qualsiasi momento visualizzare un riepilogo di informazioni sugli archivi completi e rapidi. È possibile, ad esempio, visualizzare informazioni sulla quantità di dati monitorati al momento, la quantità di dati che sono stati archiviati e al momento monitorati ma non ancora archiviati. È possibile inoltre visualizzare informazioni sulla pianificazione di archiviazioni, ad esempio le date in cui è stata eseguita l'ultima archiviazione e in cui verrà eseguita la successiva.

Visualizzazione di un riepilogo delle attività di archiviazione

È possibile visualizzare in qualsiasi momento informazioni sulle attività di archiviazione. È, ad esempio, possibile visualizzare la percentuale di file archiviati, le dimensioni dei dati monitorati, le dimensioni dei dati archiviati e di quelli monitorati ma non ancora archiviati. È possibile inoltre visualizzare le date in cui è stata eseguita l'ultima archiviazione e in cui verrà eseguita la successiva.

1. Fare clic sulla scheda **Archivio locale**.
2. Nella parte superiore della schermata, fare clic su **Riepilogo account**.

CAPITOLO 38

McAfee QuickClean

QuickClean migliora le prestazioni del computer eliminando i file superflui. Vuota il Cestino ed elimina i file temporanei, i collegamenti, i frammenti di file perduti, i file di registro, i file memorizzati nella cache, i file della cronologia del browser, la posta elettronica inviata ed eliminata, i file usati di recente, i file Active-X e i file di punto di ripristino del sistema. QuickClean protegge inoltre la privacy utilizzando il componente McAfee Shredder per eliminare in maniera sicura e definitiva gli elementi che potrebbero contenere informazioni personali sensibili, quali il nome e l'indirizzo. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

L'utilità di Deframmentazione dischi dispone i file e le cartelle nel computer in modo da assicurare che non siano sparsi, ovvero frammentati, quando vengono salvati nel disco rigido del computer. La deframmentazione periodica del disco rigido assicura che i file e le cartelle frammentate vengano consolidate per recuperarle rapidamente in un momento successivo.

Se non si desidera eseguire manualmente la manutenzione del computer è possibile pianificare l'esecuzione automatica di QuickClean e Deframmentazione dischi, come attività indipendenti, con la frequenza desiderata.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di QuickClean

Pulizia file	Consente di eliminare i file non necessari in maniera sicura ed efficiente utilizzando varie operazioni di pulizia. L'eliminazione di tali file consente di aumentare lo spazio sul disco rigido del computer e migliorarne le prestazioni.

CAPITOLO 39

Pulitura del computer

QuickClean elimina i file superflui dal computer. Vuota il Cestino ed elimina i file temporanei, i collegamenti, i frammenti di file perduti, i file di registro, i file memorizzati nella cache, i file della cronologia del browser, la posta elettronica inviata ed eliminata, i file usati di recente, i file Active-X e i file di punto di ripristino del sistema. QuickClean elimina questi elementi senza conseguenze sulle altre informazioni essenziali.

È possibile utilizzare le operazioni di pulitura di QuickClean per eliminare i file non necessari dal computer. La tabella seguente illustra le operazioni di pulitura di QuickClean.

Nome	Funzione
Pulitura del Cestino	Elimina i file del Cestino.
Pulitura dei file temporanei	Elimina i file memorizzati in cartelle temporanee.
Pulitura dei collegamenti	Elimina i collegamenti interrotti e i collegamenti a cui non è associato un programma.
Pulitura dei frammenti di file persi	Elimina i frammenti di file persi nel computer.
Pulitura del registro di sistema	Elimina le informazioni del registro di sistema di Windows® relative ai programmi che non sono più installati nel computer. Il registro è un database in cui Windows memorizza le informazioni di configurazione. Contiene i profili relativi a ciascun utente del computer nonché le informazioni relative all'hardware del sistema, i programmi installati e le impostazioni delle proprietà. Windows utilizza di continuo tali informazioni durante il funzionamento.
Pulitura della cache	Elimina i file memorizzati nella cache accumulati durante la navigazione sul Web. Tali file sono solitamente memorizzati come file temporanei in una cartella cache. Una cartella cache è un'area di memorizzazione temporanea nel computer. Per aumentare la velocità e l'efficienza della navigazione sul Web, la volta successiva che si desidera visualizzare una pagina, il browser può recuperarla dalla cache invece che dal server remoto.

Nome	Funzione
Pulitura dei cookie	Elimina i cookie. Tali file sono solitamente memorizzati come file temporanei. Un cookie è un piccolo file, che contiene informazioni che di solito comprendono il nome utente e l'ora e la data correnti, memorizzato nel computer dell'utente che naviga sul Web. I cookie vengono utilizzati principalmente dai siti Web per identificare gli utenti che si sono registrati o che hanno visitato il loro sito; tuttavia, possono anche essere una fonte di informazioni per gli hacker.
Pulitura della cronologia del browser	Elimina la cronologia del browser Web.
Pulitura posta elettronica per Outlook Express e Outlook (posta inviata ed eliminata)	Elimina la posta elettronica inviata ed eliminata da Outlook® e Outlook Express.
Pulitura dei file utilizzati di recente	Elimina i file utilizzati di recente creati con uno dei programmi seguenti: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Cronologia di Windows ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Pulitura di ActiveX	Elimina i controlli ActiveX. ActiveX è un componente software utilizzato dai programmi o dalle pagine Web per aggiungere funzionalità che si integrano e appaiono come parte normale del programma o della pagina Web. La maggior parte dei controlli ActiveX è innocua; tuttavia, alcuni potrebbero acquisire informazioni dal computer.

Nome	Funzione
Pulitura dei punti di ripristino configurazione di sistema	Elimina dal computer i vecchi punti di ripristino configurazione di sistema (ad eccezione dei più recenti). I punti di ripristino configurazione di sistema vengono creati da Windows per contrassegnare le modifiche apportate al computer, in modo che sia possibile tornare a uno stato precedente qualora si verificassero dei problemi.

In questo capitolo

Pulitura del computer

È possibile utilizzare le operazioni di pulitura di QuickClean per eliminare i file non necessari dal computer. Al termine, in **Riepilogo di QuickClean**, sarà possibile visualizzare la quantità di spazio su disco recuperata dopo la pulitura, il numero di file eliminati nonché la data e l'ora di esecuzione dell'ultima operazione di QuickClean nel computer.

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **McAfee QuickClean**, fare clic su **Avvia**.
3. Eseguire una delle seguenti operazioni:
   - Scegliere **Avanti** per accettare le operazioni di pulitura predefinite visualizzate nell'elenco.
   - Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.
   - Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.

4 Al termine dell'analisi, fare clic su **Avanti**.

5 Fare clic su **Avanti** per confermare l'eliminazione dei file.

6 Eseguire una delle seguenti operazioni:

- Fare clic su **Avanti** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
- Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi fare clic su **Avanti**. L'eliminazione definitiva dei file può richiedere molto tempo se le informazioni da cancellare sono molte.

7 Se durante la pulitura sono presenti file o elementi bloccati, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.

8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

CAPITOLO 40

Deframmentazione del computer

L'utilità di Deframmentazione dischi dispone i file e le cartelle nel computer in modo che non siano sparsi, ovvero frammentati, quando vengono salvati nel disco rigido del computer. La deframmentazione periodica del disco rigido assicura che i file e le cartelle frammentate vengano consolidate per recuperarle rapidamente in un momento successivo.

Deframmentare il computer

È possibile deframmentare il computer per migliorare l'accesso a file e cartelle e il loro recupero.

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Deframmentazione dischi**, fare clic su **Analizza**.
3. Seguire le istruzioni riportate sullo schermo.

Nota: per ulteriori informazioni su Deframmentazione dischi, vedere la Guida di Windows.

CAPITOLO 41

Pianificazione di un'attività

L'utilità di Pianificazione attività automatizza la frequenza con cui QuickClean o Deframmentazione dischi sono eseguiti nel computer. Ad esempio, è possibile pianificare un'attività di QuickClean per vuotare il Cestino ogni domenica alle 21:00, oppure un'attività di Deframmentazione dischi per deframmentare il disco rigido del computer l'ultimo giorno di ogni mese. È possibile creare, modificare o eliminare un'attività in qualsiasi momento. Perché l'attività pianificata venga eseguita, è necessario aver effettuato l'accesso al computer. Se per qualche motivo l'attività non viene eseguita, questa verrà ripianificata cinque minuti dopo l'accesso successivo.

Pianificare un'attività di QuickClean

È possibile pianificare un'attività di QuickClean per pulire automaticamente il computer utilizzando una o più operazioni di pulitura. Al termine, nella sezione **Riepilogo di QuickClean** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

   1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
   2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.

3 Immettere un nome per l'attività nella casella **Nome attività**, quindi fare clic su **Crea**.

4 Eseguire una delle seguenti operazioni:

   - Scegliere **Avanti** per accettare le operazioni di pulitura visualizzate nell'elenco.
   - Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.
   - Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.

5 Eseguire una delle seguenti operazioni:

- Fare clic su **Pianifica** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
- Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi scegliere **Pianifica**.

6 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

7 Se sono state apportate modifiche alle proprietà della pulitura dei file utilizzati di recente, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.

8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

Modificare un'attività di QuickClean

È possibile modificare un'attività pianificata di QuickClean per modificare le attività di pulitura utilizzate o la frequenza con cui un'attività viene eseguita automaticamente nel computer. Al termine, nella sezione **Riepilogo di QuickClean** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**, quindi fare clic su **Modifica**.

4 Eseguire una delle seguenti operazioni:

- Fare clic su **Avanti** per accettare le operazioni di pulitura selezionate per l'attività.
- Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.

- Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.

5 Eseguire una delle seguenti operazioni:

- Fare clic su **Pianifica** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
- Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi scegliere **Pianifica**.

6 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

7 Se sono state apportate modifiche alle proprietà della pulitura dei file utilizzati di recente, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.

8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

Eliminare un'attività di QuickClean

È possibile eliminare un'attività QuickClean pianificata se non si desidera più che sia eseguita automaticamente.

1 Aprire il riquadro Pianificazione attività.

In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**.

4 Fare clic su **Elimina**, quindi scegliere **Sì** per confermare l'eliminazione.

5 Fare clic su **Fine**.

Pianificare un'attività di deframmentazione dischi

È possibile pianificare un'attività di deframmentazione dischi per pianificare la frequenza con cui il disco rigido del computer viene deframmentato automaticamente. Al termine, nella sezione **Deframmentazione dischi** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

   1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
   2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Immettere un nome per l'attività nella casella **Nome attività**, quindi fare clic su **Crea**.

4 Eseguire una delle seguenti operazioni:

   - Fare clic su **Pianifica** per accettare l'opzione predefinita **Esegui deframmentazione anche se lo spazio disco è insufficiente**.
   - Deselezionare l'opzione **Esegui deframmentazione anche se lo spazio disco è insufficiente**, quindi fare clic su **Pianifica**.

5 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

6 Fare clic su **Fine**.

Modificare un'attività di deframmentazione dischi

È possibile modificare un'attività di deframmentazione dischi per cambiare la frequenza con cui viene eseguita automaticamente sul computer. Al termine, nella sezione **Deframmentazione dischi** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**, quindi fare clic su **Modifica**.

4 Eseguire una delle seguenti operazioni:

- Fare clic su **Pianifica** per accettare l'opzione predefinita **Esegui deframmentazione anche se lo spazio disco è insufficiente**.
- Deselezionare l'opzione **Esegui deframmentazione anche se lo spazio disco è insufficiente**, quindi fare clic su **Pianifica**.

5 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

6 Fare clic su **Fine**.

Eliminare un'attività di deframmentazione dischi

È possibile eliminare un'attività di deframmentazione dischi se non si desidera più che sia eseguita automaticamente.

1 Aprire il riquadro Pianificazione attività.

In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**.

4 Fare clic su **Elimina**, quindi scegliere **Sì** per confermare l'eliminazione.

5 Fare clic su **Fine**.

CAPITOLO 42

McAfee Shredder

McAfee Shredder cancella gli elementi, ovvero li elimina definitivamente dal disco rigido del computer. Esistono appositi strumenti informatici che consentono di recuperare le informazioni anche dopo che i file e le cartelle sono stati eliminati manualmente, il Cestino è stato svuotato oppure è stata eliminata la cartella dei file temporanei di Internet. Inoltre, è possibile recuperare un file eliminato in virtù del fatto che alcuni programmi eseguono copie temporanee e nascoste dei file aperti. Shredder protegge la privacy dell'utente eliminando in modo sicuro e definitivo i file indesiderati. È importante ricordare che i file eliminati non possono essere ripristinati.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Shredder

Eliminazione permanente di file e cartelle

Consente di eliminare gli elementi dal disco rigido in modo da rendere impossibile il recupero delle informazioni ad essi associate. Protegge la privacy dell'utente eliminando in maniera sicura e definitiva i file, le cartelle, gli elementi del Cestino e della cartella dei file temporanei Internet, nonché l'intero contenuto dei dischi del computer, quali CD riscrivibili, dischi rigidi esterni e floppy.

Eliminazione definitiva di file, cartelle e dischi

Shredder rende impossibile il recupero delle informazioni contenute nei file e nelle cartelle eliminate dal Cestino e dalla cartella dei file temporanei Internet, nemmeno con l'ausilio di strumenti specifici. Con Shredder è possibile specificare quante volte (fino a dieci) si desidera eliminare definitivamente un elemento. Un numero più elevato di tentativi di eliminazione definitiva rende più sicura l'eliminazione dei file.

Eliminare definitivamente file e cartelle

È possibile eliminare definitivamente file e cartelle dal disco rigido del computer, compresi gli elementi del Cestino e della cartella dei file temporanei Internet.

1 Aprire **Shredder**.

   In che modo?

   1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
   2. Nel riquadro di sinistra, fare clic su **Strumenti**.
   3. Fare clic su **Shredder**.

2 Nel riquadro Elimina definitivamente file e cartelle, fare clic su **Cancellare file e cartelle** nella sezione **Desidero**.

3 Nella sezione **Livello di eliminazione**, fare clic su uno dei seguenti livelli di eliminazione:

   - **Rapido**: elimina definitivamente con un passaggio gli elementi selezionati.
   - **Completo**: elimina definitivamente con sette passaggi gli elementi selezionati.
   - **Personalizzato**: elimina definitivamente con dieci passaggi gli elementi selezionati.

4 Fare clic su **Avanti**.

5 Eseguire una delle seguenti operazioni:

   - Nell'elenco **Selezionare i file da distruggere**, fare clic su **Contenuto del Cestino** o **File temporanei Internet**.
   - Fare clic su **Sfoglia**, cercare i file da eliminare definitivamente, selezionarli, quindi fare clic su **Apri**.

6 Fare clic su **Avanti**.
7 Fare clic su **Avvia**.
8 Al termine dell'operazione di eliminazione definitiva, fare clic su **Fine**.

Nota: non utilizzare alcun file fino al termine dell'operazione.

Eliminare definitivamente un intero disco

È possibile eliminare definitivamente e in modo rapido l'intero contenuto di un disco. È possibile eliminare definitivamente solo il contenuto di unità rimovibili, quali dischi rigidi esterni, CD riscrivibili e floppy.

1 Aprire **Shredder**.

   In che modo?

   1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
   2. Nel riquadro di sinistra, fare clic su **Strumenti**.
   3. Fare clic su **Shredder**.

2 Nella sezione **Desidero** del riquadro Elimina definitivamente file e cartelle, fare clic su **Cancellare un intero disco**.
3 Nella sezione **Livello di eliminazione**, fare clic su uno dei seguenti livelli di eliminazione:
   - **Rapido**: elimina definitivamente con un solo passaggio l'unità selezionata.
   - **Completo**: elimina definitivamente con sette passaggi l'unità selezionata.
   - **Personalizzato**: elimina definitivamente con dieci passaggi l'unità selezionata.

4 Fare clic su **Avanti**.
5 Nell'elenco **Selezionare il disco**, fare clic sull'unità che si desidera eliminare definitivamente.
6 Fare clic su **Avanti**, quindi su **Sì** per confermare.
7 Fare clic su **Avvia**.
8 Al termine dell'operazione di eliminazione definitiva, fare clic su **Fine**.

Nota: non utilizzare alcun file fino al termine dell'operazione.

CAPITOLO 43

McAfee Network Manager

Network Manager rappresenta graficamente i computer e altri dispositivi che costituiscono la rete domestica. Consente di gestire in modalità remota lo stato della protezione di tutti i computer gestiti in rete e quindi di risolvere le vulnerabilità della protezione segnalate sugli stessi. Se è stata installata la soluzione McAfee Total Protection, Network Manager può inoltre monitorare la rete per rilevare la presenza di intrusi (computer o dispositivi non riconosciuti o non ritenuti affidabili) che tentano di connettersi ad essa.

Prima di utilizzare Network Manager, è opportuno acquisire dimestichezza con alcune delle sue funzioni. La guida di Network Manager contiene dettagli sulla configurazione e sull'utilizzo di tali funzioni.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Network Manager

Mappa grafica della rete	Consente di visualizzare una panoramica grafica dello stato di protezione dei computer e dei dispositivi che costituiscono la rete domestica. Quando vengono apportate modifiche alla rete, ad esempio con l'aggiunta di un computer, la mappa della rete è in grado di riconoscerle. È possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli di uno qualsiasi dei dispositivi sulla mappa della rete.
Gestione remota	Consente di gestire lo stato di protezione dei computer che compongono la rete domestica. È possibile invitare un computer a diventare membro della rete gestita, monitorare lo stato di protezione del computer gestito e risolvere le vulnerabilità conosciute della protezione per un computer remoto della rete.
Monitoraggio rete	Se disponibile, consente a Network Manager di monitorare le reti e segnalare quando amici o intrusi si collegano. La funzione di monitoraggio della rete è disponibile solo se è stato acquistato McAfee Total Protection.

Informazioni sulle icone di Network Manager

Nella seguente tabella sono descritte le icone di uso comune nella mappa della rete di Network Manager.

Icona	Descrizione
	Rappresenta un computer gestito in linea
	Rappresenta un computer gestito non in linea
	Rappresenta un computer non gestito in cui è installato SecurityCenter
	Rappresenta un computer non gestito e non in linea
	Rappresenta un computer in linea in cui non è installato SecurityCenter oppure un dispositivo di rete sconosciuto
	Rappresenta un computer non in linea in cui non è installato SecurityCenter oppure un dispositivo di rete sconosciuto non in linea
	Indica che l'elemento corrispondente è protetto e connesso
	Indica che l'elemento corrispondente potrebbe richiedere l'attenzione dell'utente
	Indica che l'elemento corrispondente richiede l'attenzione immediata dell'utente
	Rappresenta un router domestico senza fili
	Rappresenta un router domestico standard
	Rappresenta Internet, quando è stata effettuata la connessione
	Rappresenta Internet, quando non è stata effettuata la connessione

CAPITOLO 44

Impostazione di una rete gestita

Per impostare una rete gestita occorre considerare affidabile la rete (nel caso non sia stato ancora fatto) e aggiungere membri (computer) alla rete. Affinché un computer possa essere gestito in modalità remota oppure sia autorizzato a gestire in modalità remota altri computer della rete, è necessario che diventi un membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative.

È possibile visualizzare i dettagli associati a uno qualsiasi degli elementi visualizzati nella mappa della rete, anche dopo aver apportato modifiche alla rete, ad esempio con l'aggiunta di un computer.

In questo capitolo

Utilizzo della mappa della rete

Quando un computer si connette alla rete, Network Manager analizza lo stato della rete al fine di determinare se sono presenti eventuali membri gestiti o non gestiti, quali sono gli attributi del router e lo stato di Internet. Se non viene rilevato alcun membro, Network Manager presume che il computer attualmente connesso sia il primo della rete, rendendolo membro gestito con autorizzazioni amministrative. Per impostazione predefinita, il nome della rete include il nome del primo computer che si connette alla rete e su cui è installato SecurityCenter. Tuttavia, è possibile rinominare la rete in qualsiasi momento.

Quando si apportano modifiche alla propria rete, se ad esempio si aggiunge un computer, è possibile personalizzare la mappa della rete. Ad esempio, è possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere degli elementi sulla mappa della rete per personalizzare la visualizzazione. È inoltre possibile visualizzare i dettagli associati a uno qualsiasi degli elementi che appaiono sulla mappa della rete.

Come accedere alla mappa della rete

La mappa della rete rappresenta graficamente i computer e i dispositivi che costituiscono la rete domestica.

- Nel menu standard o avanzato, fare clic su **Gestione rete**.

Nota: se la rete non è ancora stata considerata affidabile con McAfee Personal Firewall, verrà richiesto di farlo al primo accesso alla mappa della rete.

Come aggiornare la mappa della rete

È possibile aggiornare la mappa della rete in qualsiasi momento; ad esempio, dopo che un nuovo computer è diventato membro della rete gestita.

1. Nel menu standard o avanzato, fare clic su **Gestione rete**.
2. Fare clic su **Aggiornare la mappa della rete** nella sezione **Desidero**.

Nota: il collegamento **Aggiornare la mappa della rete** è disponibile solo se non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Come rinominare la rete

Per impostazione predefinita, il nome della rete include il nome del primo computer che si connette alla rete e su cui è installato SecurityCenter. Se si preferisce utilizzare un nome diverso, è possibile modificarlo.

1 Nel menu standard o avanzato, fare clic su **Gestione rete**.
2 Fare clic su **Rinominare la rete** nella sezione **Desidero**.
3 Digitare il nome della rete nella casella **Nome rete**.
4 Fare clic su **OK**.

Nota: il collegamento **Rinominare la rete** è disponibile solo se non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Come visualizzare o nascondere un elemento nella mappa della rete

Per impostazione predefinita, sulla mappa della rete sono visualizzati tutti i computer e i dispositivi della rete domestica. Tuttavia, se vi sono elementi nascosti, è possibile visualizzarli in qualsiasi momento. È possibile nascondere solo gli elementi non gestiti, ma non i computer gestiti.

Per...	Nel menu standard o avanzato, fare clic su Gestione rete, quindi eseguire una delle seguenti operazioni.
Nascondere un elemento nella mappa della rete	Fare clic su un elemento sulla mappa della rete, quindi su **Nascondere l'elemento** nella sezione **Desidero**. Nella finestra di dialogo di conferma, fare clic su **Sì**.
Mostrare elementi nascosti sulla mappa della rete	Nella sezione **Desidero**, fare clic su **Visualizzare gli elementi nascosti**.

Come visualizzare i dettagli di un elemento

Per visualizzare informazioni dettagliate su un elemento della rete, selezionare l'elemento dalla mappa della rete. Tra le informazioni disponibili sono inclusi il nome dell'elemento, il relativo stato della protezione nonché altri dettagli richiesti per la gestione dell'elemento.

1 Fare clic sull'icona di un elemento sulla mappa della rete.
2 Nella sezione **Dettagli** è possibile visualizzare le informazioni sull'elemento.

Aggiunta alla rete gestita

Affinché un computer sia gestito in modalità remota oppure ottenga l'autorizzazione per la gestione remota di altri computer in rete, è necessario che diventi membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative. Per garantire che vengano aggiunti alla rete solo i computer affidabili, gli utenti dei computer che concedono l'autorizzazione e quelli che la ricevono devono autenticarsi reciprocamente.

Quando un computer viene aggiunto alla rete, viene richiesto di esporne lo stato di protezione McAfee agli altri computer in rete. Se un computer accetta di esporre il proprio stato di protezione, esso diventerà un membro gestito della rete. Se un computer rifiuta di esporre il proprio stato di protezione, esso diventerà un membro non gestito della rete. I membri non gestiti della rete sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, l'invio di file o la condivisione stampanti).

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, EasyNetwork), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato a un computer in Network Manager si applica a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Come aggiungere un computer a una rete gestita

Quando si riceve un invito a diventare membro di una rete gestita, è possibile accettarlo o rifiutarlo. È anche possibile specificare se si desidera consentire agli altri computer in rete di gestire le impostazioni di protezione di questo computer.

1. Nella finestra di dialogo Rete gestita, assicurarsi che la casella di controllo **Consenti a tutti i computer della rete di gestire le impostazioni di protezione** sia selezionata.
2. Fare clic su **Aggiungi**.
   Quando si accetta l'invito vengono visualizzate due carte da gioco.
3. Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer che ha inviato l'invito a diventare membro della rete gestita.
4. Fare clic su **OK**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Annulla** nella finestra di dialogo Rete gestita.

Come invitare un computer a diventare membro della rete gestita

Se un computer viene aggiunto alla rete gestita oppure un altro computer non gestito è presente in rete, è possibile invitare tale computer a diventare membro della rete gestita. Solo i computer con autorizzazioni amministrative in rete possono invitare altri computer a diventare membri. Quando si invia l'invito, occorre inoltre specificare il livello di autorizzazione che si desidera assegnare al computer aggiunto.

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Gestire il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, effettuare una delle seguenti operazioni:
   - Fare clic su **Consenti accesso Guest a programmi della rete gestita** per consentire al computer di accedere alla rete (è possibile utilizzare questa opzione per gli utenti temporanei della rete domestica).
   - Fare clic su **Consenti accesso completo a programmi della rete gestita** per consentire al computer di accedere alla rete.

- Fare clic su **Consenti accesso con privilegi di amministratore a programmi della rete gestita** per consentire al computer di accedere alla rete con autorizzazioni amministrative. L'opzione consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.

4. Fare clic su **OK**.
   Al computer viene inviato un invito a diventare membro della rete gestita. Quando il computer accetta l'invito vengono visualizzate due carte da gioco.
5. Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer invitato a diventare membro della rete gestita.
6. Fare clic su **Consenti accesso**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Consentire al computer di diventare membro della rete può mettere a rischio altri computer, pertanto, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma.

Impostazione di computer in rete come non affidabili

Se per errore i computer sulla rete sono stati considerati affidabili, è possibile considerarli come non affidabili.

- Fare clic su **Non considerare affidabili i computer su questa rete** nella sezione **Desidero**.

Nota: il collegamento **Non considerare affidabili i computer su questa rete** non è disponibile se si dispone delle autorizzazioni amministrative e sono presenti altri computer gestiti in rete.

CAPITOLO 45

Gestione remota della rete

Dopo aver impostato la rete gestita, è possibile gestire in modalità remota i computer e i dispositivi che costituiscono la rete. È possibile gestire lo stato e i livelli di autorizzazione dei computer e dei dispositivi, nonché risolvere la maggior parte delle vulnerabilità della protezione in modalità remota.

In questo capitolo

Gestione dello stato e delle autorizzazioni

Una rete gestita prevede membri gestiti e non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di gestire lo stato della protezione McAfee. I membri non gestiti sono di solito computer Guest che desiderano accedere ad altre funzioni della rete (ad esempio, l'invio di file o la condivisione di stampanti). Un computer non gestito può essere invitato a diventare un computer gestito in qualsiasi momento da un altro computer gestito con autorizzazioni amministrative per la rete. Analogamente, un computer gestito con autorizzazioni amministrative può rendere non gestito un altro computer gestito in qualsiasi momento.

Ai computer gestiti sono associate autorizzazioni amministrative, complete o Guest. Le autorizzazioni amministrative consentono al computer gestito di amministrare lo stato della protezione di tutti gli altri computer gestiti in rete, nonché di concedere agli altri computer di diventare membri della rete. Le autorizzazioni complete e Guest consentono a un computer solo di accedere alla rete. È possibile modificare il livello di autorizzazione di un computer in qualsiasi momento.

Poiché una rete gestita può comprendere anche dei dispositivi (ad esempio i router), è possibile gestire anche questi ultimi mediante Network Manager. È inoltre possibile configurare e modificare le proprietà di visualizzazione di un dispositivo sulla mappa della rete.

Come gestire lo stato della protezione di un computer

Se lo stato della protezione del computer non è gestito in rete (il computer non è membro oppure è un membro non gestito), è possibile inviare una richiesta di gestione.

1. Fare clic sull'icona di un computer non gestito sulla mappa della rete.
2. Fare clic su **Gestire il computer** nella sezione **Desidero**.

Come interrompere la gestione dello stato della protezione di un computer

È possibile interrompere la gestione dello stato della protezione di un computer gestito nella rete privata; tuttavia, il computer diventa un membro non gestito e non sarà possibile gestirne lo stato della protezione in modalità remota.

1. Fare clic sull'icona di un computer gestito sulla mappa della rete.
2. Fare clic su **Interrompere la gestione del computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Come modificare le autorizzazioni di un computer gestito

È possibile modificare le autorizzazioni di un computer gestito in qualsiasi momento. Ciò consente di modificare i computer che possono gestire lo stato della protezione di altri computer della rete.

1 Fare clic sull'icona di un computer gestito sulla mappa della rete.

2 Fare clic su **Modificare i permessi per il computer** nella sezione **Desidero**.

3 Nella finestra di dialogo di modifica dei permessi, selezionare o deselezionare la casella di controllo per determinare se il computer selezionato e altri computer sulla rete gestita possono gestire reciprocamente il rispettivo stato della protezione.

4 Fare clic su **OK**.

Come gestire una periferica

È possibile gestire una periferica eseguendo l'accesso alla relativa pagina Web di amministrazione dalla mappa di rete.

1 Fare clic sull'icona di una periferica sulla mappa della rete.

2 Fare clic su **Gestire la periferica** nella sezione **Desidero**. Il browser Web verrà aperto e verrà visualizzata la pagina Web di amministrazione della periferica.

3 Nel browser Web, fornire i dati di accesso e configurare le impostazioni di protezione della periferica.

Nota: se la periferica è un router o un punto di accesso senza fili protetto con Wireless Network Security, per configurare le impostazioni di protezione della periferica è necessario utilizzare McAfee Wireless Network Security.

Modifica delle proprietà di visualizzazione di una periferica

Quando si modificano le proprietà di visualizzazione di una periferica è possibile modificare il nome della periferica visualizzato e specificare se si tratta di un router senza fili.

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Modificare le proprietà della periferica** nella sezione **Desidero**.
3. Per specificare il nome della periferica visualizzato, digitare un nome nella casella **Nome**.
4. Per specificare il tipo di periferica, fare clic su **Router** se si tratta di un router standard oppure **Router wireless** se si tratta di un router senza fili.
5. Fare clic su **OK**.

Risoluzione delle vulnerabilità della protezione

I computer gestiti con autorizzazioni amministrative possono gestire lo stato della protezione McAfee di altri computer gestiti sulla rete e risolvere le vulnerabilità segnalate in modalità remota. Ad esempio, se lo stato della protezione McAfee di un computer gestito indica che VirusScan è disattivato, un altro computer gestito con autorizzazioni amministrative può attivare VirusScan in modalità remota.

Quando si risolvono le vulnerabilità della protezione in modalità remota, Network Manager è in grado di risolvere gran parte dei problemi segnalati. Tuttavia, alcune vulnerabilità della protezione possono richiedere un intervento manuale sul computer locale. In tal caso, Network Manager risolve i problemi su cui è possibile intervenire in modalità remota, quindi chiede all'utente di risolvere i problemi rimanenti effettuando l'accesso a SecurityCenter sul computer vulnerabile e attenendosi ai suggerimenti forniti. In alcuni casi, per correggere il problema si suggerisce di installare la versione più recente di SecurityCenter sul computer remoto o sui computer in rete.

Risolvere vulnerabilità della protezione

È possibile utilizzare Network Manager per risolvere gran parte delle vulnerabilità della protezione sui computer gestiti remoti. Ad esempio, se VirusScan è disattivato su un computer remoto, è possibile attivarlo.

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Visualizzare lo stato della protezione dell'elemento nella sezione **Dettagli**.
3. Fare clic su **Risolvere vulnerabilità della protezione** nella sezione **Desidero**.
4. Dopo aver risolto i problemi di protezione, fare clic su **OK**.

Nota: benché Network Manager risolva automaticamente gran parte delle vulnerabilità della protezione, per l'esecuzione di alcune operazioni potrebbe essere necessario avviare SecurityCenter sul computer vulnerabile e attenersi ai suggerimenti forniti.

Come installare il software di protezione McAfee sui computer remoti

Se su uno o più computer della rete non si utilizza una versione recente di SecurityCenter, lo stato della protezione di tali computer non potrà essere gestito in modalità remota. Se si desidera gestire questi computer in modalità remota, è necessario installare una versione recente di SecurityCenter su ciascuno di essi.

1. Assicurarsi di attenersi a queste istruzioni sul computer che si desidera gestire in modalità remota.
2. È necessario avere a portata di mano le informazioni per l'accesso di McAfee, ossia l'indirizzo di posta elettronica e la password utilizzati nel corso della prima attivazione del software McAfee.
3. In un browser, andare al sito Web McAfee, effettuare l'accesso e fare clic su **Account**.
4. Individuare il prodotto che si desidera installare, fare clic sul relativo pulsante **Download** e seguire le istruzioni riportate sullo schermo.

Suggerimento: per informazioni sulle modalità di installazione del software di protezione McAfee su computer remoti, aprire la mappa della rete e fare clic su **Proteggere i PC** nella sezione **Desidero**.

CAPITOLO 46

Monitoraggio delle reti

Se è stata installata la soluzione McAfee Total Protection, Network Manager esegue il monitoraggio delle reti per rilevare anche l'eventuale presenza di intrusi. Ogni volta che un computer o un dispositivo sconosciuto si collega alla rete, l'utente riceverà un avviso, in modo da poter stabilire se tale computer o dispositivo è un amico o un intruso. Un amico è un computer o dispositivo riconosciuto e considerato affidabile, un intruso è un computer o dispositivo non riconosciuto e non considerato affidabile. Se si contrassegna un computer o dispositivo come amico, sarà possibile decidere se ricevere un avviso ogni volta che tale amico si connette alla rete. Se il computer o dispositivo viene contrassegnato come intruso, l'utente riceverà automaticamente un avviso a ogni tentativo di connessione alla rete.

La prima volta che si effettua la connessione alla rete dopo aver installato questa versione di Total Protection o aver eseguito l'aggiornamento, il computer o dispositivo verrà automaticamente contrassegnato come amico e in futuro i tentativi di connessione alla rete dello stesso non verranno notificati all'utente. Dopo tre giorni, l'utente inizierà a ricevere avvisi relativi a ogni tentativo di accesso effettuato da un computer o dispositivo sconosciuto, in modo che possa contrassegnarli personalmente.

Nota: il monitoraggio della rete è una funzione di Network Manager disponibile solo con McAfee Total Protection. Per ulteriori informazioni su Total Protection, visitare il sito Web di McAfee.

In questo capitolo

Come bloccare il monitoraggio reti

Se l'utente disattiva il monitoraggio della rete, McAfee non sarà più in grado di avvisarlo se degli intrusi si connettono alla rete domestica o a qualsiasi altra rete a cui l'utente si connette.

1 Aprire il riquadro Configurazione di Internet e rete.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro Home di SecurityCenter, fare clic su **Internet e rete**.
3. Nella sezione Internet e rete, fare clic su **Configura**.

2 In **Monitoraggio rete**, fare clic su **Disattiva**.

Come riattivare le notifiche del monitoraggio di rete

Benché sia possibile, si sconsiglia di disattivare le notifiche del monitoraggio di rete. In tal caso, McAfee non sarà più in grado di avvisare l'utente quando intrusi o computer sconosciuti si connettono alla rete. Se si disattivano inavvertitamente tali notifiche (ad esempio, se si seleziona la casella di controllo **Non visualizzare questo messaggio in futuro** nella finestra di un avviso), sarà possibile riattivarle in qualsiasi momento.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi informativi**.

3 Nel riquadro Avvisi informativi, assicurarsi che le seguenti caselle di controllo siano deselezionate:

- **Non visualizzare avvisi quando nuovi PC o dispositivi si collegano alla rete**
- **Non visualizzare avvisi quando intrusi si collegano alla rete**
- **Non visualizzare avvisi per gli amici di cui solitamente desidero ricevere notifica**
- **Non visualizzare promemoria al rilevamento di PC o dispositivi sconosciuti**
- **Non visualizzare avvisi quando McAfee ha completato il rilevamento di nuovi amici**

4 Fare clic su **OK**.

Come contrassegnare un computer come intruso

Contrassegnare un computer o dispositivo in rete come intruso se non è riconosciuto o considerato affidabile. Si riceverà automaticamente un avviso ogni volta che l'intruso tenta di connettersi alla rete.

1 Nel menu standard o avanzato, fare clic su **Gestione rete**.
2 Fare clic su un elemento sulla mappa della rete.
3 In **Desidero**, fare clic su **Contrassegnare come amico o intruso**.
4 Nella finestra di dialogo, fare clic su **Un intruso**.

Come contrassegnare un computer come amico

Contrassegnare un computer o dispositivo in rete come amico solo se è riconosciuto e considerato affidabile. Quando si contrassegna un computer o dispositivo come amico, è anche possibile decidere se ricevere un avviso ogni volta che questo si connette alla rete.

1 Nel menu standard o avanzato, fare clic su **Gestione rete**.
2 Fare clic su un elemento sulla mappa della rete.
3 In **Desidero**, fare clic su **Contrassegnare come amico o intruso**.
4 Nella finestra di dialogo, fare clic su **Un amico**.
5 Per ricevere un avviso a ogni tentativo dell'amico di connettersi alla rete, selezionare la casella di controllo **Avvisami quando questo computer o dispositivo si collega alla rete**.

Come interrompere il rilevamento di nuovi amici

Dopo aver effettuato la connessione a una rete con questa versione di Total Protection installata, per i primi tre giorni ciascun computer o dispositivo verrà automaticamente contrassegnato come amico, per il quale l'utente non desidera ricevere alcuna notifica. È possibile interrompere il processo di designazione automatica in qualsiasi momento nel corso di questi tre giorni, ma non sarà possibile riavviarlo in seguito.

1 Nel menu standard o avanzato, fare clic su **Gestione rete**.
2 Nella sezione **Desidero**, fare clic su **Interrompere il rilevamento di nuovi amici**.

CAPITOLO 47

McAfee EasyNetwork

EasyNetwork consente la condivisione protetta di file, semplifica i trasferimenti di file e permette la condivisione delle stampanti tra computer della rete domestica. Tuttavia, per accedere alle relative funzioni è necessario aver installato EasyNetwork sui computer in rete.

Prima di utilizzare EasyNetwork, è opportuno acquisire dimestichezza con alcune delle funzioni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di EasyNetwork.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di EasyNetwork

EasyNetwork fornisce le funzioni riportate di seguito.

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra i computer in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer che dispongono di accesso completo o con privilegi di amministratore alla rete gestita (membri) possono condividere file o accedere a file condivisi da altri membri.

Trasferimento di file

È possibile inviare file ad altri computer che dispongono di accesso completo o con privilegi di amministratore alla rete gestita (membri). Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, che rappresenta il percorso di archiviazione temporaneo per tutti i file inviati da altri computer della rete.

Condivisione automatica di stampanti

Dopo che l'utente è diventato membro di una rete gestita, è possibile condividere tutte le stampanti locali collegate al computer con altri membri, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

CAPITOLO 48

Impostazione di EasyNetwork

Per utilizzare EasyNetwork è necessario avviarlo e diventare membro di una rete gestita. Solo in seguito sarà possibile condividere, cercare e inviare file ad altri computer in rete. È anche possibile condividere le stampanti. Sarà possibile decidere di abbandonare la rete in qualsiasi momento.

In questo capitolo

Come avviare EasyNetwork

È possibile avviare EasyNetwork dal menu Start di Windows oppure facendo clic sulla relativa icona sul desktop.

- Nel menu **Start**, scegliere **Programmi**, quindi **McAfee** e fare clic su **McAfee EasyNetwork**.

Suggerimento: è anche possibile avviare EasyNetwork facendo doppio clic sull'icona di McAfee EasyNetwork sul desktop.

Aggiunta di un membro alla rete gestita

Se SecurityCenter non è disponibile su nessun computer in rete a cui è connesso l'utente, quest'ultimo diventerà membro della rete e gli verrà chiesto di stabilire se si tratta di rete affidabile. Poiché è il primo computer a diventare membro della rete, il nome del computer in uso viene incluso nel nome della rete, che potrà tuttavia essere rinominata in qualsiasi momento.

Quando un computer stabilisce una connessione alla rete, richiede agli altri computer in rete l'autorizzazione a diventarne membro. Alla richiesta è possibile acconsentire da qualsiasi computer con autorizzazioni amministrative in rete. La persona che concede le autorizzazioni può inoltre determinare il livello di autorizzazione del computer che diventa membro della rete, ad esempio, Guest (solo trasferimento file) oppure completo/con privilegi di amministratore (trasferimento e condivisione file). In EasyNetwork, i computer che dispongono di accesso con privilegi di amministratore possono consentire l'accesso ad altri computer e gestire autorizzazioni (alzare o abbassare il livello dei computer) mentre i computer con accesso completo non sono in grado di eseguire attività amministrative di questo tipo.

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, Network Manager), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato al computer in EasyNetwork viene applicato a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta di un membro alla rete

Quando un computer si connette a una rete affidabile per la prima volta dopo l'installazione di EasyNetwork, viene visualizzato un messaggio che chiede al computer se intende diventare membro di una rete gestita. Se il computer accetta di diventarlo, verrà inviata una richiesta a tutti gli altri computer in rete che dispongono di accesso con privilegi di amministratore. Tale richiesta deve essere accettata prima che il computer possa condividere stampanti o file oppure inviare e copiare file in rete. Al primo computer in rete vengono automaticamente concesse le autorizzazioni amministrative.

1. Nella finestra File condivisi, fare clic su **Aggiungi il computer alla rete**.
   Quando un computer con privilegi di amministratore in rete acconsente alla richiesta, viene visualizzato un messaggio in cui viene chiesto se si intende consentire al computer in uso e agli altri della rete di gestire le impostazioni di protezione reciproche.
2. Per consentire al computer in uso e agli altri computer di rete di gestire le reciproche impostazioni di protezione, fare clic su **OK**, altrimenti fare clic su **Annulla**.
3. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, quindi fare clic su **OK**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Annulla** nella finestra di dialogo di conferma.

Autorizzazione di accesso alla rete

Quando un computer chiede di diventare membro di una rete gestita, viene inviato un messaggio agli altri computer in rete che dispongono di accesso con privilegi di amministratore. Il primo computer a rispondere diventa quello dell'utente che concede le autorizzazioni e, come tale, l'utente di questo computer sarà responsabile della scelta del tipo di accesso: Guest, completo o con privilegi di amministratore.

1. Nell'avviso, fare clic sul livello di accesso appropriato.
2. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, effettuare una delle seguenti operazioni:
   - Fare clic su **Consenti accesso Guest a programmi della rete gestita** per consentire l'accesso al computer di accedere alla rete (è possibile utilizzare questa opzione per gli utenti temporanei della rete domestica).
   - Fare clic su **Consenti accesso completo a programmi della rete gestita** che consente al computer di accedere alla rete.
   - Fare clic su **Consenti accesso con privilegi di amministratore a programmi della rete gestita** che consente al computer di accedere alla rete con autorizzazioni amministrative. Consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.
3. Fare clic su **OK**.
4. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer, quindi fare clic su **Concedi accesso**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer, significa che si è verificata una violazione della protezione sulla rete gestita. Poiché concedere a questo computer l'accesso alla rete può mettere a rischio il computer in uso, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma della protezione.

Rinominare la rete

Per impostazione predefinita, il nome della rete include il nome del primo computer diventato membro della rete; tuttavia, è possibile modificarlo in qualsiasi momento. Quando si rinomina la rete, è possibile modificare la relativa descrizione visualizzata in EasyNetwork.

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, digitare il nome della rete nella casella **Nome di rete**.
3. Fare clic su **OK**.

Abbandono della rete gestita

Se l'utente diventato membro di una rete non intende più essere tale, può abbandonare la rete. Dopo aver abbandonato una rete, è sempre possibile chiedere nuovamente di essere aggiunti; tuttavia, sarà necessario ottenere di nuovo l'autorizzazione. Per ulteriori informazioni sull'adesione, vedere Aggiunta di un membro alla rete gestita (pagina 244).

Come abbandonare una rete gestita

È possibile abbandonare una rete gestita di cui si era precedentemente diventati membro.

1. Disconnettere il computer dalla rete.
2. In EasyNetwork, nel menu **Strumenti**, scegliere **Abbandona rete**.
3. Nella finestra di dialogo Abbandona rete, selezionare il nome della rete che si desidera abbandonare.
4. Fare clic su **Abbandona rete**.

CAPITOLO 49

Condivisione e invio di file

EasyNetwork semplifica la condivisione e l'invio di file tra gli altri computer presenti in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri.

Nota: l'eventuale condivisione di un numero elevato di file può incidere sulle risorse del computer.

In questo capitolo

Condivisione di file

Solo i computer membri della rete gestita (che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri. Se si condivide una cartella, vengono condivisi tutti i file in essa contenuti e le relative sottocartelle, tuttavia la condivisione delle cartelle aggiunte successivamente non avviene automaticamente. Una volta eliminati, file e cartelle condivisi vengono rimossi dalla finestra File condivisi. È possibile interrompere la condivisione di un file in qualsiasi momento.

Per accedere a un file condiviso, aprirlo direttamente da EasyNetwork oppure copiarlo sul computer e quindi aprirlo. Se l'elenco dei file condivisi è troppo lungo per individuare il file desiderato, è possibile effettuare la ricerca dei file.

Nota: i file condivisi con EasyNetwork non sono accessibili da altri computer mediante Esplora risorse, in quanto la condivisione dei file EasyNetwork viene eseguita mediante connessioni protette.

Condivisione di un file

Quando si condivide un file, questo viene reso disponibile a tutti i membri che dispongono di accesso alla rete gestita, sia esso completo o con privilegi di amministratore.

1 In Esplora risorse, individuare il file che si desidera condividere.

2 Trascinare il file dal percorso in Esplora risorse nella finestra File condivisi in EasyNetwork.

Suggerimento: è anche possibile condividere un file facendo clic su **Condividi file** nel menu **Strumenti**. Nella finestra di dialogo Condividi, passare alla cartella in cui è memorizzato il file che si desidera condividere, selezionarlo e fare clic su **Condividi**.

Interruzione della condivisione di un file

Se un file viene condiviso sulla rete gestita, è possibile interrompere la condivisione in qualsiasi momento. Quando si interrompe la condivisione di un file, gli altri membri della rete gestita non possono accedervi.

1 Nel menu **Strumenti**, scegliere **Interrompi condivisione file**.

2 Nella finestra di dialogo Interrompi condivisione file, selezionare il file che non si desidera più condividere.

3 Fare clic su **OK**.

Copia di un file condiviso

Un utente copia un file condiviso in modo da poterne disporre anche quando non è più condiviso. È possibile copiare un file condiviso proveniente da un qualsiasi computer della rete gestita.

- Trascinare un file dalla finestra File condivisi in EasyNetwork in un percorso di Esplora risorse o sul desktop di Windows.

Suggerimento: è anche possibile copiare un file condiviso selezionandolo in EasyNetwork, quindi facendo clic su **Copia in** nel menu **Strumenti**. Nella finestra di dialogo Copia in, passare alla cartella in cui si desidera copiare il file, selezionarlo e fare clic su **Salva**.

Ricerca di un file condiviso

È possibile ricercare un file di cui si è eseguita la condivisione oppure che è stato condiviso da qualsiasi altro membro della rete. Nel momento in cui vengono digitati i criteri di ricerca, EasyNetwork visualizza i risultati corrispondenti nella finestra File condivisi.

1. Nella finestra File condivisi, fare clic su **Cerca**.
2. Fare clic sull'opzione appropriata (pagina 252) nell'elenco **Contiene**.
3. Digitare, tutto o in parte, il nome del file o del percorso nell'elenco **Nome file o percorso**.
4. Fare clic sul tipo di file (pagina 252) nell'elenco **Tipo**.
5. Negli elenchi **Da** e **A**, fare clic sulle date che rappresentano l'intervallo temporale in cui è stato creato il file.

Criteri di ricerca

Nelle tabelle seguenti sono descritti i criteri che è possibile specificare quando si esegue la ricerca di file condivisi.

Nome o percorso del file

Contiene	Descrizione
Contiene tutte le parole	Consente di cercare il nome di un file o di un percorso contenente tutte le parole specificate nell'elenco **Nome file o percorso**, in qualsiasi ordine.
Contiene una qualsiasi delle parole	Consente di cercare il nome di un file o di un percorso contenente una qualsiasi delle parole specificate nell'elenco **Nome file o percorso**.
Contiene la stringa esatta	Consente di cercare il nome di un file o di un percorso contenente esattamente la stringa specificata nell'elenco **Nome file o percorso**.

Tipo di file

Tipo	Descrizione
Qualsiasi	Consente di cercare tutti i tipi di file condivisi.
Documento	Consente di cercare tutti i documenti condivisi.
Immagine	Consente di cercare tutti i file immagine condivisi.
Video	Consente di cercare tutti i file video condivisi.
Audio	Consente di cercare tutti i file audio condivisi.
Compressi	Consente di cercare tutti i file compressi (ad esempio, i file .zip)

Invio di file ad altri computer

È possibile inviare file ad altri computer purché siano membri della rete gestita. Prima di inviare un file, EasyNetwork verifica che il computer che lo riceve abbia sufficiente spazio su disco.

Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, un percorso di archiviazione temporaneo per i file inviati da altri computer della rete. Se durante la ricezione EasyNetwork è aperto, il file viene immediatamente visualizzato nella casella dei file in arrivo; in caso contrario viene visualizzato un messaggio nell'area di notifica all'estremità destra della barra delle applicazioni. Se non si desidera ricevere messaggi di notifica (se interrompono le proprie attività, ad esempio) è possibile disattivare questa funzione. Qualora nella casella dei file in arrivo esista già un file con lo stesso nome, il nuovo file viene rinominato con un suffisso numerico. I file restano nella casella finché l'utente li accetta, cioè finché vengono copiati sul computer in uso.

Invio di un file a un altro computer

È possibile inviare un file a un altro computer nella rete gestita senza condividerlo. Prima che un utente del computer destinatario possa visualizzare il file, sarà necessario salvarlo in un percorso locale. Per ulteriori informazioni, vedere Accettazione di un file da un altro computer (pagina 254).

1 In Esplora risorse, individuare il file che si desidera inviare.

2 Trascinare il file dal percorso in Esplora risorse in un'icona attiva del computer in EasyNetwork.

Suggerimento: per inviare più file a un computer premere CTRL mentre li si seleziona. Per inviare i file è inoltre possibile fare clic su **Invia** nel menu **Strumenti**, selezionare i file e fare clic su **Invia**.

Accettazione di un file proveniente da un altro computer

Se un altro computer della rete gestita invia un file all'utente, è necessario accettarlo salvandolo sul computer. Se EasyNetwork non è in esecuzione durante l'invio del file al computer in uso, l'utente riceverà un messaggio nell'area di notifica all'estremità destra della barra delle applicazioni. Fare clic sul messaggio di notifica per aprire EasyNetwork e accedere al file.

- Fare clic su **Ricevuto**, quindi trascinare il file dalla casella dei file in arrivo di EasyNetwork in una cartella di Esplora risorse.

Suggerimento: è anche possibile ricevere un file da un altro computer selezionandolo nella casella dei file in arrivo di EasyNetwork e facendo clic su **Accetta** nel menu **Strumenti**. Nella finestra di dialogo Accetta nella cartella, passare alla cartella in cui si desidera salvare i file in ricezione, effettuare la selezione e fare clic su **Salva**.

Ricezione di una notifica all'invio di un file

È possibile ricevere un messaggio di notifica quando un altro computer della rete gestita invia un file. Se EasyNetwork non è in esecuzione, il messaggio di notifica viene visualizzato nell'area di notifica all'estremità destra della barra delle applicazioni.

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, selezionare la casella di controllo **Avvisa quando è in corso l'invio di file da un altro computer**.
3. Fare clic su **OK**.

CAPITOLO 50

Condivisione di stampanti

Dopo che l'utente è diventato membro di una rete gestita, EasyNetwork condivide le stampanti locali collegate al computer in uso, utilizzando il nome della stampante come nome della stampante condivisa, EasyNetwork rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

Se è stato configurato un driver per stampare mediante un server di stampa di rete (ad esempio, un server di stampa USB senza fili), EasyNetwork considera la stampante come locale e la condivide in rete. È anche possibile interrompere la condivisione di una stampante in qualsiasi momento.

In questo capitolo

Uso delle stampanti condivise

EasyNetwork rileva le stampanti condivise dagli altri computer della rete. In caso di rilevamento di una stampante remota non connessa al computer, quando EasyNetwork viene aperto per la prima volta, nella finestra File condivisi viene visualizzato il collegamento **Stampanti di rete disponibili**. In questo modo l'utente potrà installare le stampanti disponibili o disinstallare quelle già connesse al computer nonché aggiornare l'elenco delle stampanti per assicurarsi di visualizzare informazioni aggiornate.

Se invece è connesso alla rete gestita ma non ne è diventato membro, l'utente potrà accedere alle stampanti condivise mediante il pannello di controllo delle stampanti di Windows.

Interruzione della condivisione di una stampante

Se si interrompe la condivisione di una stampante, i membri non potranno utilizzarla.

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Gestione stampanti di rete, fare clic sul nome della stampante che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Installazione di una stampante di rete disponibile

Se l'utente è membro della rete gestita, può accedere alle stampanti condivise in rete; tuttavia, sarà necessario installare il driver utilizzato dalla stampante. Se il proprietario della stampante ne interrompe la condivisione, gli utenti non saranno in grado di utilizzarla.

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Stampanti di rete disponibili, fare clic sul nome di una stampante.
3. Fare clic su **Installa**.

Riferimento

Nel Glossario dei termini sono elencati e illustrati i termini relativi alla protezione più comunemente utilizzati nei prodotti McAfee.

Glossario

8

802.11

Insieme di standard per la trasmissione di dati su una rete senza fili. 802.11 è comunemente noto come Wi-Fi.

802.11a

Estensione di 802.11 che consente la trasmissione di dati fino a 54 Mbps nella banda dei 5 GHz. Nonostante la velocità di trasmissione sia superiore rispetto a 802.11b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che consente la trasmissione di dati fino a 11 Mbps nella banda dei 2,4 GHz. Nonostante la velocità di trasmissione sia inferiore rispetto a 802.11b, la distanza coperta è superiore.

802.1x

Standard per l'autenticazione sulle reti cablate e senza fili. 802.1x è comunemente utilizzato con la rete senza fili 802.11. Vedere anche autenticazione (pagina 259).

A

account di posta elettronica standard

Vedere POP3 (pagina 264).

archiviazione

Creazione di una copia dei file importanti su CD, DVD, unità USB, disco rigido esterno o unità di rete. Confronta backup (pagina 259).

archivio protetto password

Area di memorizzazione protetta per le password personali che consente di memorizzare le password in modo tale che nessun altro utente, compreso un amministratore, possa accedervi.

attacco brute force

Metodo utilizzato dagli hacker per trovare password o chiavi di crittografia provando ogni possibile combinazione di caratteri fino a violare la crittografia.

attacco di tipo dictionary

Tipo di attacco di forza bruta che utilizza parole comuni per provare a scoprire una password.

attacco di tipo man-in-the-middle

Metodo di intercettazione ed eventuale modifica dei messaggi tra due parti senza che una delle parti venga a conoscenza della violazione del collegamento della comunicazione.

attacco DoS (Denial of Service)

Tipo di attacco contro un computer, un server o una rete che rallenta o arresta il traffico su una rete. Si verifica quando una rete è inondata da una quantità di ulteriori richieste talmente elevata che il normale traffico viene rallentato o completamente interrotto. Un attacco DoS sovraccarica la destinazione con false richieste di connessione, in modo che la destinazione ignori le richieste legittime.

autenticazione

Processo di verifica dell'identità digitale del mittente di una comunicazione elettronica.

B

backup

Creazione di una copia dei file importanti in genere su un server online protetto. Confronta archiviazione (pagina 258).

browser

Programma utilizzato per visualizzare le pagine Web su Internet. Tra i browser Web più conosciuti si annoverano Microsoft Internet Explorer e Mozilla Firefox.

C

cache

Area di memorizzazione temporanea sul computer per dati a cui si è effettuato l'accesso spesso o di recente. Ad esempio, per aumentare la velocità e l'efficienza della navigazione sul Web, la volta successiva che si desidera visualizzare una pagina, il browser può recuperarla dalla cache invece che dal server remoto.

cavallo di Troia, trojan

Programma che non esegue repliche, ma provoca danni o compromette la protezione del computer. In genere, un cavallo di Troia viene inviato tramite posta elettronica da un utente a un altro. L'invio tramite posta non avviene automaticamente. È anche possibile scaricare il cavallo di Troia a propria insaputa da un sito Web o tramite una rete peer-to-peer.

Cestino

Cestino della spazzatura fittizio per i file e le cartelle eliminati in Windows.

chiave

Serie di lettere e numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre della chiave. Vedere anche WEP (pagina 270), WPA (pagina 270), WPA2 (pagina 271), WPA2-PSK (pagina 271), WPA-PSK (pagina 271).

client

Programma eseguito su PC o workstation che richiede un server per l'esecuzione di alcune operazioni. Ad esempio, un client di posta elettronica è un'applicazione che consente l'invio e la ricezione di messaggi di posta elettronica.

client di posta elettronica

Programma eseguito sul computer per l'invio e la ricezione di posta elettronica, ad esempio Microsoft Outlook.

collegamento

File che contiene solo il percorso di un altro file sul computer.

compressione

Processo che comprime i file in un formato tale da ridurre al minimo lo spazio richiesto per la memorizzazione o la trasmissione.

condivisione

Operazione che consente ai destinatari di un messaggio di posta elettronica di accedere ai file di backup selezionati per un periodo limitato di tempo. Quando si condivide un file, la copia di backup del file viene inviata ai destinatari del messaggio di posta elettronica specificati. I destinatari ricevono un messaggio di posta elettronica da Backup e ripristino in cui viene segnalato che i file sono stati condivisi. Nel messaggio di posta elettronica è riportato anche un collegamento ai file condivisi.

controllo ActiveX

Componente software utilizzato dai programmi o dalle pagine Web per aggiungere funzionalità che appaiono come parte normale del programma o della pagina Web. La maggior parte dei controlli ActiveX sono innocui; tuttavia, alcuni potrebbero acquisire informazioni dal computer.

cookie

Piccolo file di testo utilizzato da molti siti Web per memorizzare le informazioni sulle pagine visitate, memorizzato nel computer dell'utente che naviga sul Web. Può contenere informazioni sull'accesso o sulla registrazione, informazioni sul carrello o le preferenze dell'utente. I cookie vengono utilizzati principalmente dai siti Web per identificare gli utenti che si sono registrati o che hanno visitato il loro sito Web; tuttavia, possono anche essere una fonte di informazioni per gli hacker.

crittografia

Metodo di codifica delle informazioni affinché persone non autorizzate non possano accedervi. Quando i dati vengono codificati, il processo utilizza una "chiave" e algoritmi matematici. Le informazioni crittografate non possono venire decrittografate senza la chiave corretta. I virus utilizzano talvolta la crittografia per evitare di essere rilevati.

DAT

File di definizione rilevamento, detti anche file delle firme elettroniche, contenenti le definizioni che identificano, rilevano e riparano virus, trojan horse, spyware, adware e altri programmi potenzialmente indesiderati (PUP, Potentially Unwanted Program).

dialer

Software che reindirizza le connessioni Internet verso un corrispondente diverso dal provider di servizi Internet (ISP, Internet Service Provider) predefinito dell'utente per aggiungere ulteriori addebiti per la connessione a un fornitore di contenuti o ad altra terza parte.

disco rigido esterno

Disco rigido collegato all'esterno del computer.

DNS

Domain Name System. Sistema di database che converte un indirizzo IP, ad esempio 11.2.3.44, in un nome di dominio, ad esempio www.mcafee.com.

dominio

Sottorete locale o descrittore per siti su Internet. Su una rete locale (LAN), un dominio è una sottorete costituita da computer client e server controllati da un database di protezione. Su Internet, un dominio è parte di ogni indirizzo Web. Ad esempio, in www.mcafee.com, mcafee è il dominio.

E

elenco degli elementi affidabili

Elenco di elementi considerati affidabili e non rilevati. Elementi quali, ad esempio, programmi potenzialmente indesiderati o modifiche del registro, dovranno essere rimossi dall'elenco se considerati erroneamente affidabili o se si desidera verificarne di nuovo la presenza.

elenco indirizzi autorizzati

Elenco di siti Web o di indirizzi di posta elettronica considerati sicuri. I siti Web in un elenco indirizzi autorizzati sono quelli a cui gli utenti hanno il permesso di accedere. Gli indirizzi di posta elettronica in un elenco indirizzi autorizzati provengono da origini affidabili di cui si desidera ricevere i messaggi. Confronta elenco indirizzi bloccati (pagina 261).

elenco indirizzi bloccati

In Anti-Spam, elenco di indirizzi di posta elettronica da cui non si desidera ricevere messaggi perché si ritiene che i messaggi saranno indesiderati. Nell'anti-phishing, elenco di siti Web considerati dannosi. Confronta elenco indirizzi attendibili (pagina 261).

ESS

Extended Service Set. Due o più reti che formano un'unica sottorete.

evento

In un programma o sistema di computer, un incidente o un'occorrenza che può essere rilevata dal software di protezione, in base a criteri predefiniti. Un evento genera solitamente un'azione, quale l'invio di una notifica o l'aggiunta di una voce a un registro eventi.

F

file temporanei

File creati in memoria o sul disco dal sistema operativo o da un altro programma e che vengono utilizzati durante una sessione per essere quindi eliminati.

firewall

Sistema progettato (hardware, software o entrambi) per impedire l'accesso non autorizzato a o da una rete privata. I firewall vengono utilizzati di frequente per impedire a utenti di Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una rete Intranet. Tutti i messaggi in entrata o in uscita su Internet passano attraverso il firewall, il quale esamina tutti i messaggi e blocca quelli non conformi ai criteri di protezione specificati.

frammenti di file

Porzioni di un file sparsi su un disco. La frammentazione dei file si verifica quando si aggiungono o eliminano file e può inoltre rallentare le prestazioni del computer.

gateway integrato

Dispositivo che combina le funzioni di punto di accesso (AP), router e firewall. Alcuni dispositivi includono persino funzionalità avanzate di protezione e bridging.

gruppo di classificazione del contenuto

In Controllo genitori, gruppo di età a cui appartiene un utente. Il contenuto viene reso disponibile o bloccato in base al gruppo di classificazione del contenuto al quale appartiene l'utente. I gruppi di classificazione del contenuto comprendono: minori di 6 anni, 6-9 anni, 10-13 anni, 14-18 anni, maggiori di 18 anni.

H

hotspot

Limite geografico coperto da un punto di accesso (AP) Wi-Fi (802.11). Gli utenti che entrano in un hotspot con un laptop senza fili possono connettersi a Internet, a condizione che l'hotspot sia un Web beacon, ovvero che pubblicizzi la propria presenza, e non sia richiesta l'autenticazione. Gli hotspot sono spesso situati in zone molto popolate, quali ad esempio gli aeroporti.

indirizzo IP

Indirizzo Internet Protocol. Indirizzo utilizzato per identificare un computer o un dispositivo su una rete TCP/IP. L'indirizzo IP presenta il formato di un indirizzo dinamico a 32 bit espresso con quattro numeri separati da punti. Ogni numero può essere compreso tra 0 e 255, ad esempio 192.168.1.100.

indirizzo MAC

Indirizzo Media Access Control. Numero di serie univoco assegnato a un dispositivo fisico (NIC, Network Interface Card) che accede alla rete.

intranet

Rete privata di computer, generalmente all'interno di un'organizzazione, alla quale possono accedere solo gli utenti autorizzati.

L

LAN

Local Area Network. Rete di computer che si estende in un'area relativamente ridotta, ad esempio un singolo edificio. I computer su una rete LAN possono comunicare tra loro e condividere le risorse quali stampanti e file.

larghezza di banda

Quantità di dati trasmettibili (velocità effettiva) in un determinato lasso di tempo.

launchpad

Componente dell'interfaccia U3 che funge da punto di partenza per l'avvio e la gestione dei programmi USB U3.

M

MAC (Message Authentication Code)

Codice di protezione utilizzato per crittografare i messaggi trasmessi tra i computer. Il messaggio viene accettato se il computer riconosce il codice decrittografato come valido.

MAPI

Messaging Application Programming Interface. Specifica di interfaccia di Microsoft che consente a differenti programmi di workgroup e messaggistica (tra cui posta elettronica, casella vocale e fax) di collaborare attraverso un singolo client, ad esempio il client di Exchange.

mappa di rete

Rappresentazione grafica dei computer e dei componenti che costituiscono la rete domestica.

MSN

Microsoft Network. Gruppo di servizi basati sul Web offerti da Microsoft Corporation, tra cui motore di ricerca, posta elettronica, messaggistica immediata e portale.

N

NIC

Network Interface Card. Scheda che si inserisce in un laptop o in altro dispositivo e consente la connessione del dispositivo alla LAN.

nodo

Singolo computer connesso a una rete.

P

password

Codice, in genere costituito da lettere e numeri, utilizzato per ottenere l'accesso a un computer, a un programma o a un sito Web.

percorsi monitorati

Cartelle sul computer monitorate da Backup e ripristino.

phishing

Metodo per ottenere senza autorizzazione informazioni personali, quali password, numeri di codice fiscale e dettagli della carta di credito, inviando messaggi di posta elettronica contraffatti che sembrano provenire da origini affidabili, quali banche o società legittime. In genere, nei messaggi di tipo phishing viene richiesto ai destinatari di fare clic sul collegamento nel messaggio per verificare o aggiornare i dettagli del contatto o le informazioni sulla carta di credito.

plugin, plug-in

Programma software di piccole dimensioni che aggiunge funzionalità o migliora un software di dimensioni maggiori. Ad esempio, i plug-in consentono al browser Web di accedere ai file incorporati nei documenti HTML il cui formato non verrebbe normalmente riconosciuto, quali file di animazione, audio e video, e quindi di eseguirli.

POP3

Post Office Protocol 3. Interfaccia tra un programma client di posta elettronica e il server di posta elettronica. La maggior parte degli utenti domestici utilizza account e-mail POP3, noti anche come account e-mail standard.

popup

Piccole finestre che vengono visualizzate davanti ad altre finestre sullo schermo del computer. Le finestre popup sono spesso utilizzate nei browser Web per visualizzare annunci pubblicitari.

porta

Posizione hardware per il passaggio di dati verso e fuori da un dispositivo informatico. Nei personal computer sono disponibili svariati tipi di porte, incluse porte interne per la connessione di unità disco, monitor e tastiere, oltre a porte esterne per la connessione di modem, stampanti, mouse e altre periferiche.

posta elettronica

Posta elettronica. Messaggi inviati e ricevuti a livello elettronico su una rete di computer. Vedere anche Web mail (pagina 270).

PPPoE

Point-to-Point Protocol Over Ethernet (protocollo punto a punto su Ethernet). Metodo di utilizzo del protocollo punto a punto su Ethernet come mezzo di trasporto.

programma potenzialmente indesiderato (PUP)

Programma software che potrebbe essere indesiderato, anche se è possibile che gli utenti abbiano acconsentito a scaricarlo. Può alterare le impostazioni relative alla protezione o alla privacy del computer in cui viene installato. I programmi PUP possono includere, ma non necessariamente, spyware, adware e dialer e possono essere scaricati con un programma desiderato dall'utente.

protocollo

Insieme di regole che consentono ai computer o ai dispositivi di scambiare dati. In un'architettura di rete a più livelli (modello Open Systems Interconnection), ogni livello dispone di protocolli propri che specificano come avviene la comunicazione a tale livello. Per comunicare con altri computer, il computer o dispositivo in uso deve utilizzare il protocollo corretto. Vedere anche OSI (Open Systems Interconnection).

proxy

Computer o software che separa una rete da Internet, presentando un solo indirizzo di rete ai siti esterni. Rappresentando tutti i computer interni, il proxy protegge le identità di rete pur continuando a fornire l'accesso a Internet. Vedere anche server proxy (pagina 267).

pubblicazione

Processo il cui scopo è rendere un file di backup disponibile a tutti su Internet. È possibile accedere ai file pubblicati eseguendo una ricerca nella libreria di Backup e ripristino.

punto di accesso (AP, Access Point)

Dispositivo di rete, noto comunemente come router senza fili, che si collega a un hub o switch Ethernet per ampliare la gamma fisica di servizi a un utente senza fili. Quando gli utenti senza fili si collegano con i dispositivi portatili, la trasmissione passa da un punto di accesso all'altro per mantenere la connettività.

punto di accesso pericoloso

Punto di accesso non autorizzato. I punti di accesso pericolosi possono essere installati su una rete aziendale protetta per concedere l'accesso alla rete a utenti non autorizzati. Possono inoltre essere creati per consentire all'autore dell'attacco di condurre un attacco di tipo man-in-the-middle.

punto di ripristino configurazione di sistema

Istantanea (immagine) del contenuto della memoria del computer o di un database. Windows crea dei punti di ripristino periodicamente e in caso di eventi significativi del sistema, ad esempio se si installa un programma o un driver. È inoltre possibile creare e denominare i propri punti di ripristino in qualsiasi momento.

quarantena

Isolamento forzato di un file o una cartella sospettata di contenere un virus, posta indesiderata, contenuto sospetto o programmi potenzialmente indesiderati, in modo che le cartelle i i file non possano essere aperti o eseguiti.

R

RADIUS

Remote Access Dial-In User Service. Protocollo che consente l'autenticazione utente, di solito in un contesto di accesso remoto. Inizialmente definito per l'uso con i server di accesso remoto dial-in, viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x del segreto condiviso di un utente di una WLAN. Vedere anche segreto condiviso.

Registro di sistema

Database utilizzato da Windows per memorizzare le informazioni sulla configurazione per ogni utente del computer, l'hardware di sistema, i programmi installati e le impostazioni delle proprietà. Il database si suddivide in chiavi, per le quali vengono impostati valori. I programmi indesiderati possono modificare il valore delle chiavi del Registro di sistema o crearne di nuove, per eseguire codice dannoso.

rete

Insieme di sistemi basati su IP (quali router, commutatori, server e firewall) raggruppati come unità logica. Ad esempio, una "rete finanziaria" potrebbe includere tutti i server, i router e i sistemi utilizzati da un reparto finanziario. Vedere anche rete domestica (pagina 266).

rete domestica

Due o più computer connessi in un ambiente domestico per la condivisione dei file e dell'accesso a Internet. Vedere anche LAN (pagina 263).

roaming

Spostamento da un'area coperta da un punto di accesso (AP) a un'altra senza interruzione di servizio o perdita di connettività.

rootkit

Insieme di strumenti (programmi) che concedono a un utente l'accesso a livello di amministratore a un computer o rete di computer. Possono comprendere spyware e altri programmi potenzialmente indesiderati che possono rappresentare un rischio per la protezione dei dati presenti sul computer o per la privacy.

router

Dispositivo di rete che inoltra pacchetti di dati da una rete all'altra. I router leggono ogni pacchetto in ingresso e decidono come inoltrarlo in base agli indirizzi di origine e di destinazione, nonché alle attuali condizioni di traffico. A volte il router è denominato anche punto di accesso (AP).

S

scansione in tempo reale

Processo di verifica della presenza di virus e altre attività in file e cartelle al momento dell'accesso da parte dell'utente o del computer.

scansione su richiesta

Esame programmato di file, applicazioni o dispositivi di rete selezionati per trovare una minaccia, una vulnerabilità o altro codice potenzialmente indesiderato. Può essere eseguita immediatamente, a un'ora programmata o a intervalli regolari. Confronta scansione all'accesso. Vedere anche vulnerabilità.

scheda di rete senza fili

Dispositivo che fornisce la funzionalità senza fili a un computer o PDA. È collegato mediante una porta USB, uno slot per scheda PC (CardBus), uno slot per scheda di memoria o internamente al bus PCI.

scheda senza fili PCI

Peripheral Component Interconnect. Scheda senza fili connessa mediante uno slot di espansione PCI all'interno del computer.

scheda senza fili USB

Scheda senza fili connessa mediante una porta USB del computer.

script

Elenco di comandi in grado di essere eseguiti in modo automatico, ovvero senza l'intervento dell'utente. Diversamente dai programmi, in genere gli script sono memorizzati nel rispettivo testo normale e vengono compilati a ogni esecuzione. Anche le macro e i file batch sono detti script.

segreto condiviso

Stringa o chiave, normalmente una password, condivisa tra due parti in comunicazione prima di avviare la comunicazione. Viene utilizzato per proteggere le porzioni più riservate dei messaggi RADIUS. Vedere anche RADIUS (pagina 265).

server

Computer o programma che accetta le connessioni da altri computer o programmi e restituisce le apposite risposte. Ad esempio, il programma di posta elettronica si collega a un server di posta elettronica ogni volta che l'utente invia o riceve messaggi e-mail.

server proxy

Componente del firewall che gestisce il traffico Internet da e verso una LAN (Local Area Network). Un server proxy consente di migliorare le prestazioni fornendo i dati richiesti frequentemente, ad esempio una pagina Web, e di filtrare ed eliminare le richieste non considerate appropriate, quali le richieste di accesso non autorizzato ai file proprietari.

sincronizzazione

Risoluzione di eventuali incoerenze tra i file di backup e quelli memorizzati sul computer locale. La sincronizzazione è necessaria quando la versione di un file presente nell'archivio del backup in linea è più recente rispetto a quella del file memorizzato negli altri computer.

smart drive

Vedere unità USB (pagina 269).

SMTP

Simple Mail Transfer Protocol. Protocollo TCP/IP per l'invio di messaggi da un computer a un altro su una rete. Questo protocollo è utilizzato su Internet per instradare i messaggi di posta elettronica.

sovraccarico del buffer

Condizione che si verifica quando programmi o processi sospetti tentano di memorizzare in un buffer (area di memorizzazione temporanea dei dati) una quantità di dati superiore al limite consentito. Un sovraccarico del buffer danneggia la memoria o sovrascrive i dati presenti nei buffer adiacenti.

spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, inclusa la presa di controllo della sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta indesiderati in modo da impedire la corretta individuazione dei mittenti.

SSID

Service Set Identifier. Token, o chiave segreta, che identifica una rete Wi-Fi (802.11). Il token SSID viene impostato dall'amministratore della rete e deve essere fornito dagli utenti che desiderano accedere alla rete.

SSL

Secure Sockets Layer. Protocollo sviluppato da Netscape per la trasmissione di documenti privati su Internet. Il protocollo SSL utilizza una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Gli URL che richiedono una connessione SSL iniziano con HTTPS anziché con HTTP.

SystemGuard

Avvisi di McAfee che rilevano e notificano la presenza di modifiche non autorizzate sul computer.

T

testo cifrato

Testo crittografato. Il testo cifrato è illeggibile finché non viene convertito in testo normale, ovvero viene decrittografato. Vedere anche crittografia (pagina 260).

testo normale

Testo non crittografato. Vedere anche crittografia (pagina 260).

tipi di file monitorati

Tipi di file (ad esempio doc, xls), di cui Backup e ripristino esegue il backup o che memorizza negli archivi all'interno dei percorsi monitorati.

TKIP

Temporal Key Integrity Protocol (pronuncia ti-kip). Parte dello standard di crittografia 802.11i per le reti LAN wireless. TKIP costituisce la nuova generazione di WEP, utilizzato per proteggere le reti LAN wireless 802.11. TKIP fornisce la combinazione di chiavi per pacchetto, un controllo dell'integrità del messaggio e un meccanismo di reimpostazione delle chiavi, correggendo in tal modo i difetti di WEP.

U

U3

You: Simplified, Smarter, Mobile. Piattaforma che consente di eseguire programmi per Windows 2000 o Windows XP direttamente su un'unità USB. L'iniziativa U3 è stata fondata nel 2004 da M-Systems e SanDisk e consente agli utenti di eseguire programmi U3 su computer Windows senza installare o memorizzare dati e impostazioni sul computer stesso.

unità di rete

Unità disco o nastro collegata a un server su una rete e condivisa da più utenti. Le unità di rete sono spesso note come "unità remote".

Unità USB

Piccola unità di memoria che si collega alla porta USB del computer. Un'unità USB funge da piccolo disco rigido, semplificando il trasferimento di file da un computer all'altro.

URL

Uniform Resource Locator. Formato standard per gli indirizzi Internet.

USB

Universal Serial Bus. Connettore standard nel settore presente nei computer più moderni, che connette più dispositivi, tra cui tastiere e mouse, webcam, scanner e stampanti.

virus

Programma in grado di copiare se stesso e infettare un computer senza autorizzazione o a insaputa dell'utente.

VPN

Virtual Private Network. Rete privata per le comunicazioni configurata tramite una rete host, quale Internet. I dati che passano attraverso una connessione VPN vengono crittografati e sono dotati di funzionalità di protezione affidabili.

wardriver

Persona che tenta di intercettare le reti Wi-Fi (802.11) girando per le città con un computer Wi-Fi e alcuni componenti hardware o software speciali.

Web bug

Piccoli file grafici che si incorporano autonomamente nelle pagine HTML e consentono a un'origine non autorizzata di impostare cookie sul computer dell'utente. I cookie possono quindi trasmettere dati all'origine non autorizzata. I Web bug sono anche chiamati "Web beacon", "pixel tag", "GIF trasparenti" o "GIF invisibili".

Web mail

Posta basata sul Web. Servizio di posta elettronica a cui si accede principalmente tramite un browser Web anziché tramite un client di posta elettronica basato sul computer, quale Microsoft Outlook. Vedere anche posta elettronica (pagina 264).

WEP

Wired Equivalent Privacy. Protocollo di crittografia e autenticazione definito come parte dello standard Wi-Fi (802.11). Le versioni iniziali sono basate su crittografia RC4 e sono caratterizzate da una notevole vulnerabilità. WEP tenta di fornire la protezione crittografando i dati su onde radio, in modo che siano protetti durante la trasmissione fra due punti. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi

Wireless Fidelity. Termine utilizzato da Wi-Fi Alliance per fare riferimento a qualsiasi tipo di rete 802.11.

Wi-Fi Alliance

Organizzazione costituita dai principali fornitori di hardware e software senza fili. Wi-Fi Alliance si impegna a certificare tutti i prodotti basati sullo standard 802.11 per assicurare l'interoperabilità e a promuovere il termine Wi-Fi come marchio globale in tutti i mercati per tutti i prodotti LAN senza fili basati su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere lo sviluppo di questo settore.

Wi-Fi Certified

Prodotto che deve essere testato e approvato da Wi-Fi Alliance. I prodotti Wi-Fi Certified devono garantire l'interoperabilità anche se provengono da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un punto di accesso di qualunque marca con hardware client di qualsiasi altra marca, purché siano certificati.

WLAN

Wireless Local Area Network. Rete LAN che utilizza una connessione senza fili. Una WLAN utilizza onde radio ad alta frequenza anziché fili per consentire ai computer di comunicare tra loro.

worm

Virus che si diffonde creando duplicati di se stesso su altre unità, sistemi o reti. Un worm di mass-mailing necessita dell'intervento dell'utente per diffondersi, ad esempio tramite l'apertura di un allegato o l'esecuzione di un file scaricato. La maggior parte degli attuali virus di posta elettronica è costituita da worm. Un worm che si trasmette automaticamente non necessita dell'intervento dell'utente per propagarsi. Tra i worm che si trasmettono automaticamente sono inclusi Blaster e Sasser.

WPA

Wi-Fi Protected Access. Standard di specifiche che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso dei sistemi LAN senza fili, esistenti e futuri. Progettato per funzionare sull'hardware esistente come upgrade software, WPA è derivato dallo standard 802.11i ed è compatibile con esso. Se correttamente installato, garantisce agli utenti della LAN senza fili un elevato livello di protezione dei dati e che l'accesso alla rete venga effettuato solo da utenti autorizzati.

WPA-PSK

Speciale modalità WPA progettata per gli utenti privati che non richiedono una protezione avanzata a livello enterprise e non hanno accesso a server di autenticazione. Utilizzando questa modalità, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Pre-Shared Key, chiave già condivisa) e deve cambiare regolarmente la passphrase su ciascun punto di accesso e computer senza fili. Vedere anche WPA2-PSK (pagina 271), TKIP (pagina 268).

WPA2

Aggiornamento dello standard di protezione WPA, basato sullo standard 802.11i.

WPA2-PSK

Modalità WPA speciale, simile a WPA-PSK e basata sullo standard WPA2. Una funzione comune di WPA2-PSK è che i dispositivi spesso supportano più modalità di crittografia (ad esempio AES, TKIP) contemporaneamente, mentre i dispositivi più obsoleti supportano generalmente solo una singola modalità di crittografia alla volta (ossia, tutti i client devono utilizzare la stessa modalità di crittografia).

Informazioni su McAfee

McAfee, Inc., con sede centrale a Santa Clara, California, leader globale nella gestione dei rischi associati alla protezione e nella prevenzione delle intrusioni, offre soluzioni e servizi dinamici e affidabili che proteggono sistemi e reti in tutto il mondo. Grazie alla sua insuperata esperienza in materia di protezione e al suo impegno in termini di innovazione, McAfee offre agli utenti privati, alle aziende, al settore pubblico e ai provider di servizi la capacità di bloccare gli attacchi, di impedire le interruzioni dei servizi e di controllare e migliorare continuamente la protezione dei loro sistemi.

Licenza

AVVISO AGLI UTENTI: LEGGERE ATTENTAMENTE IL TESTO DEL CONTRATTO RELATIVO ALLA LICENZA ACQUISTATA, CHE STABILISCE LE CONDIZIONI GENERALI DI FORNITURA PER L'UTILIZZO DEL SOFTWARE CONCESSO IN LICENZA. NEL CASO IN CUI NON SI SAPPIA CON ESATTEZZA CHE TIPO DI LICENZA È STATA ACQUISTATA, CONSULTARE I DOCUMENTI DI VENDITA E ALTRE AUTORIZZAZIONI CONNESSE O LA DOCUMENTAZIONE RELATIVA ALL'ORDINE DI ACQUISTO CHE ACCOMPAGNA LA CONFEZIONE DEL SOFTWARE O CHE È STATA RICEVUTA SEPARATAMENTE IN RELAZIONE ALL'ACQUISTO MEDESIMO (SOTTO FORMA DI OPUSCOLO, FILE CONTENUTO NEL CD DEL PRODOTTO O FILE DISPONIBILE SUL SITO WEB DAL QUALE È STATO ESEGUITO IL DOWNLOAD DEL SOFTWARE). SE NON SI ACCETTANO ALCUNI O TUTTI I TERMINI DEL CONTRATTO, ASTENERSI DALL'INSTALLARE IL SOFTWARE. SE PREVISTO DAL CONTRATTO, L'UTENTE POTRÀ RESTITUIRE IL PRODOTTO A MCAFEE, INC. O AL PUNTO VENDITA IN CUI È STATO ACQUISTATO ED ESSERE INTERAMENTE RIMBORSATO.

CAPITOLO 51

Assistenza clienti e supporto tecnico

SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. I problemi critici di protezione richiedono un intervento immediato e comportano il passaggio dello stato della protezione a rosso. I problemi non critici di protezione non richiedono un intervento immediato e, a seconda del tipo di problema, possono influire sullo stato della protezione. Per raggiungere uno stato della protezione verde, è necessario risolvere tutti i problemi critici e risolvere oppure ignorare tutti i problemi non critici. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee. Per ulteriori informazioni sul tecnico virtuale di McAfee, consultare la relativa Guida.

Se il software di protezione è stato acquistato da un partner o fornitore diverso da McAfee, aprire un browser Web e accedere a www.mcafeeaiuto.com. Quindi, da Collegamenti partner, selezionare il partner o il fornitore per accedere al tecnico virtuale di McAfee.

Nota: per installare ed eseguire il tecnico virtuale di McAfee, è necessario accedere al computer come amministratore di Windows. In caso contrario, il tecnico virtuale di McAfee potrebbe non essere in grado di risolvere i problemi. Per informazioni sull'accesso come amministratore di Windows, vedere la Guida di Windows. In Windows Vista™, viene visualizzata una richiesta all'avvio del tecnico virtuale di McAfee. In questo caso, fare clic su **Accetto**. Il tecnico virtuale non è disponibile con Mozilla® Firefox.

In questo capitolo

Utilizzo del tecnico virtuale di McAfee

Analogamente a un addetto del supporto tecnico, il tecnico virtuale raccoglie informazioni sui programmi SecurityCenter in uso al fine di fornire assistenza nella risoluzione dei problemi di protezione del computer. Il tecnico virtuale, quando attivato, verifica il corretto funzionamento dei programmi SecurityCenter in uso. Se rileva problemi, il tecnico virtuale offre la possibilità di risolverli automaticamente oppure fornisce indicazioni dettagliate su di essi. Effettuate tutte le operazioni, il tecnico virtuale comunica i risultati delle analisi e, se necessario, consente di ottenere ulteriore assistenza dal supporto tecnico di McAfee.

Per preservare la protezione e l'integrità del computer e dei file in uso, il tecnico virtuale non raccoglie dati personali che possano identificare l'utente.

Nota: per ulteriori informazioni, accedere al tecnico virtuale e fare clic sull'icona **?**.

Come avviare il tecnico virtuale

Il tecnico virtuale raccoglie informazioni sui programmi SecurityCenter in uso al fine di fornire assistenza nella risoluzione dei problemi di protezione. Per garantire la privacy, il tecnico virtuale non raccoglie alcun dato personale in grado di identificare gli utenti del computer.

1. Nella sezione **Attività comuni**, fare clic su **Tecnico virtuale di McAfee**.
2. Seguire le istruzioni visualizzate sullo schermo per scaricare e avviare il tecnico virtuale.

Consultare le tabelle seguenti per informazioni sui siti di assistenza e download McAfee nel proprio paese o area geografica, comprese le Guide dell'utente.

Supporto e download

Paese/area geografica	Assistenza McAfee	Download McAfee
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasile	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (francese)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Canada (inglese)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Cina (cinese semplificato)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Corea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Danimarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlandia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Francia	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Germania	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Giappone	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Grecia	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Messico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norvegia	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polonia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portogallo	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Regno Unito	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp

Repubblica Ceca	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Russia	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slovacchia	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Spagna	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Stati Uniti	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Svezia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turchia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Ungheria	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp

Guide dell'utente di McAfee Total Protection

Paese/area geografica	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Cina (cinese semplificato)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Grecia	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Paesi Bassi	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Regno Unito	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Russia	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovacchia	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Ungheria	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf

Guide dell'utente di McAfee Internet Security

Paese/area geografica	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf

Canada (francese)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Cina (cinese semplificato)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Paesi Bassi	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Regno Unito	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Russia	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovacchia	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf

Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Ungheria	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf

Guide dell'utente di McAfee VirusScan Plus

Paese/area geografica	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Cina (cinese semplificato)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Paesi Bassi	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf

Portogallo	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Regno Unito	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Russia	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovacchia	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Ungheria	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf

Guide dell'utente di McAfee VirusScan

Paese/area geografica	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Cina (cinese semplificato)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf

Germania	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Paesi Bassi	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Regno Unito	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Russia	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovacchia	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Ungheria	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf

Consultare le tabelle seguenti per informazioni sul Centro minacce McAfee e sui siti contenenti informazioni virus nel proprio paese o area geografica.

Paese/area geografica	Quartier generale della sicurezza	Informazioni sui virus
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasile	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (francese)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (inglese)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Cina (cinese semplificato)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Corea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Danimarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francia	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Germania	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Giappone	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Grecia	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Messico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norvegia	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Paesi Bassi	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Polonia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portogallo	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Regno Unito	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo

Repubblica Ceca	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Russia	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovacchia	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Spagna	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Stati Uniti	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Svezia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turchia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Ungheria	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo

Consultare la seguente tabella per informazioni sui siti HackerWatch nel proprio paese o area geografica.

Paese/area geografica	HackerWatch
Australia	www.hackerwatch.org
Brasile	www.hackerwatch.org/?lang=pt-br
Canada (francese)	www.hackerwatch.org/?lang=fr-ca
Canada (inglese)	www.hackerwatch.org
Cina (cinese semplificato)	www.hackerwatch.org/?lang=zh-cn
Corea	www.hackerwatch.org/?lang=ko
Danimarca	www.hackerwatch.org/?lang=da
Finlandia	www.hackerwatch.org/?lang=fi
Francia	www.hackerwatch.org/?lang=fr
Germania	www.hackerwatch.org/?lang=de
Giappone	www.hackerwatch.org/?lang=jp
Grecia	www.hackerwatch.org/?lang=el
Italia	www.hackerwatch.org/?lang=it
Messico	www.hackerwatch.org/?lang=es-mx

Norvegia	www.hackerwatch.org/?lang=no
Paesi Bassi	www.hackerwatch.org/?lang=nl
Polonia	www.hackerwatch.org/?lang=pl
Portogallo	www.hackerwatch.org/?lang=pt-pt
Regno Unito	www.hackerwatch.org
Repubblica Ceca	www.hackerwatch.org/?lang=cs
Russia	www.hackerwatch.org/?lang=ru
Slovacchia	www.hackerwatch.org/?lang=sk
Spagna	www.hackerwatch.org/?lang=es
Stati Uniti	www.hackerwatch.org
Svezia	www.hackerwatch.org/?lang=sv
Taiwan	www.hackerwatch.org/?lang=zh-tw
Turchia	www.hackerwatch.org/?lang=tr
Ungheria	www.hackerwatch.org/?lang=hu

Indice

D

E

F

G

H

I

L

T

U

V

W